Part II — Galois Theory

Based on lectures by C. Birkar

Notes taken by Dexter Chua

Michaelmas 2015

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

Groups, Rings and Modules is essential

Field extensions, tower law, algebraic extensions; irreducible polynomials and relation with simple algebraic extensions. Finite multiplicative subgroups of a field are cyclic. Existence and uniqueness of splitting fields. [6]

Existence and uniqueness of algebraic closure. [1]

Separability. Theorem of primitive element. Trace and norm. [3]

Normal and Galois extensions, automorphic groups. Fundamental theorem of Galois theory. [3]

Galois theory of finite fields. Reduction mod p. [2]

Cyclotomic polynomials, Kummer theory, cyclic extensions. Symmetric functions. Galois theory of cubics and quartics. [4]

Solubility by radicals. Insolubility of general quintic equations and other classical problems. [3]

Artin's theorem on the subfield fixed by a finite group of automorphisms. Polynomial invariants of a finite group; examples. [2]

Contents

0 Introduction **3**

1 Solving equations **4**

2 Field extensions **7**
2.1 Field extensions 7
2.2 Ruler and compass constructions 12
2.3 K-homomorphisms and the Galois Group 14
2.4 Splitting fields 16
2.5 Algebraic closures 19
2.6 Separable extensions 22
2.7 Normal extensions 30
2.8 The fundamental theorem of Galois theory 33
2.9 Finite fields 36

3 Solutions to polynomial equations **40**
3.1 Cyclotomic extensions 40
3.2 Kummer extensions 44
3.3 Radical extensions 47
3.4 Solubility of groups, extensions and polynomials 50
3.5 Insolubility of general equations of degree 5 or more 54

4 Computational techniques **59**
4.1 Reduction mod p 59
4.2 Trace, norm and discriminant 62

0 Introduction

The most famous result of Galois theory is that there is no general solution to polynomial equations of degree 5 or above in terms of radicals. However, this result was, in fact, proven before Galois theory existed, and goes under the name of the *Abel–Ruffini theorem*. What Galois theory does provides is a way to decide whether a given polynomial has a solution in terms of radicals, as well as a nice way to prove this result.

However, Galois theory is more than equation solving. In fact, the *fundamental theorem of Galois theory*, which is obviously an important theorem in Galois theory, has completely nothing to do with equation solving. Instead, it is about group theory.

In modern days, Galois theory is often said to be the study of field extensions. The idea is that we have a field K, and then add more elements to get a field L. When we want to study solutions to polynomial equations, what we add is the roots of the polynomials. We then study the properties of this field extension, and in some cases, show that this field extension cannot be obtained by just adding radicals.

For certain "nice" field extensions $K \subseteq L$, we can assign to it the *Galois group* $\mathrm{Gal}(L/K)$. In general, given any group G, we can find subgroups of G. On the other hand, given a field extension $K \subseteq L$, we can try to find some intermediate field F that can be fitted into $K \subseteq F \subseteq L$. The key idea of Galois theory is that these two processes are closely related — we can establish a one-to-one correspondence between the subgroups of G and the intermediate fields F.

Moreover, many properties of (intermediate) field extensions correspond to analogous ideas in group theory. For example, we have the notion of normal subgroups, and hence there is an analogous notion of normal extensions. Similarly, we have soluble extensions (i.e. extensions that can be obtained by adding radicals), and these correspond to "soluble groups". In Galois theory, we will study how group-theoretic notions and field-theoretic notions interact.

Nowadays, Galois theory is an important field in mathematics, and finds its applications in number theory, algebraic geometry and even cryptography.

1 Solving equations

Galois theory grew of of the desire to *solve equations*. In particular, to solve polynomial equations. To begin with, we will come up with general solutions to polynomial equations of up to degree 4. However, this is the best we can do, as we will later show in the course — there is no general solution to polynomial equations of degree 5 or above.

Before we start, we will define some notations that we will frequently use.

If R is a ring, then $R[t]$ is the polynomial ring over R in the variable t. Usually, we take $R = \mathbb{Q}$ and consider polynomials $f(t) \in \mathbb{Q}[t]$. The objective is then to find roots to the equation $f(t) = 0$. Often, we want to restrict our search domain. For example, we might ask if there is a root in $\mathbb{Q}$. We will thus use $\mathrm{Root}_f(X)$ to denote the set of all roots of f in X.

Linear equations

Suppose that $f = t + a \in \mathbb{Q}[t]$ (with $a \in \mathbb{Q}$). This is easy to solve — we have $\mathrm{Root}_f(\mathbb{Q}) = \{-a\}$.

Quadratic equations

Consider a simple quadratic $f = t^2 + 1 \in \mathbb{Q}[t]$. Then $\mathrm{Root}_f(\mathbb{Q}) = \emptyset$ since the square of all rationals are positive. However, in the complex plane, we have $\mathrm{Root}_f(\mathbb{C}) = \{\sqrt{-1}, -\sqrt{-1}\}$.

In general, let $f = t^2 + at + b \in \mathbb{Q}[t]$. Then as we all know, the roots are given by

$$\mathrm{Root}_f(\mathbb{C}) = \left\{ \frac{-a \pm \sqrt{a^2 - 4b}}{2} \right\}$$

Cubic equations

Let $f = t^3 + c \in \mathbb{Q}[t]$. The roots are then

$$\mathrm{Root}_f(\mathbb{C}) = \{\sqrt[3]{-c}, \mu\sqrt[3]{-c}, \mu^2\sqrt[3]{-c}\},$$

where $\mu = \frac{-1+\sqrt{-3}}{2}$ is the 3rd root of unity. Note that μ is defined by the equation $\mu^3 - 1 = 0$, and satisfies $\mu^2 + \mu + 1 = 0$.

In general, let $f = t^3 + at^2 + bt + c \in \mathbb{Q}[t]$, and let $\mathrm{Root}_f(\mathbb{C}) = \{\alpha_1, \alpha_2, \alpha_3\}$, not necessarily distinct.

Our objective is to solve $f = 0$. Before doing so, we have to make it explicit what we mean by "solving" the equation. As in solving the quadratic, we want to express the roots α_1, α_2 and α_3 in terms of "radicals" involving a, b and c.

Unlike the quadratic case, there is no straightforward means of coming up with a general formula. The result we currently have is the result of many many years of hard work, and the substitutions we make seemingly come out of nowhere. However, after a lot of magic, we will indeed come up with a general formula for it.

We first simplify our polynomial by assuming $a = 0$. Given any polynomial $f = t^3 + at^2 + bt + c$, we know a is the negative of the sum of the roots. So we can increase each root by $\frac{a}{3}$ so that the coefficient of t^2 vanishes. So we perform

the change of variables $t \mapsto t - \frac{a}{3}$, and get rid of the coefficient of t^2. So we can assume $a = 0$.

Let μ be as above. Define

$$\beta = \alpha_1 + \mu\alpha_2 + \mu^2\alpha_3$$
$$\gamma = \alpha_1 + \mu^2\alpha_2 + \mu\alpha_3$$

These are the *Lagrange resolvers*. We obtain

$$\beta\gamma = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + (\mu + \mu^2)(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3)$$

Since $\mu^2 + \mu + 1 = 0$, we have $\mu^2 + \mu = -1$. So we can simplify to obtain

$$= (\alpha_1 + \alpha_2 + \alpha_3)^2 - 3(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3)$$

We have $\alpha_1 + \alpha_2 + \alpha_3 = -a = 0$, while $b = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3$. So

$$= -3b$$

Cubing, we obtain

$$\beta^3\gamma^3 = -27b^3.$$

On the other hand, recalling again that $\alpha_1 + \alpha_2 + \alpha_3 = 0$, we have

$$\begin{aligned}\beta^3 + \gamma^3 &= (\alpha_1 + \mu\alpha_2 + \mu^2\alpha_3)^3 + (\alpha_1 + \mu^2\alpha_2 + \mu\alpha_3)^3 + (\alpha_1 + \alpha_2 + \alpha_3)^3 \\ &= 3(\alpha_1^3 + \alpha_2^3 + \alpha_3^3) + 18\alpha_1\alpha_2\alpha_3\end{aligned}$$

We have $\alpha_1\alpha_2\alpha_3 = -c$, and since $\alpha_i^3 + b\alpha_i + c = 0$ for all i, summing gives $\alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3c = 0$. So

$$= -27c$$

Hence, we obtain

$$(t - \beta^3)(t - \gamma^3) = t^2 + 27ct - 27b^3.$$

We already know how to solve this equation using the quadratic formula. We obtain

$$\{\beta^3, \gamma^3\} = \left\{\frac{-27c \pm \sqrt{(27c)^2 + 4 \times 27b^3}}{2}\right\}$$

We now have β^3 and γ^3 in terms of radicals. So we can find β and γ in terms of radicals. Finally, we can solve for α_i using

$$0 = \alpha_1 + \alpha_2 + \alpha_3$$
$$\beta = \alpha_1 + \mu\alpha_2 + \mu^2\alpha_3$$
$$\gamma = \alpha_1 + \mu^2\alpha_2 + \mu\alpha_3$$

In particular, we obtain

$$\alpha_1 = \frac{1}{3}(\beta + \gamma)$$
$$\alpha_2 = \frac{1}{3}(\mu^2\beta + \mu\gamma)$$
$$\alpha_3 = \frac{1}{3}(\mu\beta + \mu^2\gamma)$$

So we can solve a cubic in terms of radicals.

This was a lot of magic involved, and indeed this was discovered through a lot of hard work throughout many many years. This is also not a very helpful result since we have no idea where these substitutions came from and why they intuitively work.

Quartic equations

Assume $f = t^4 + at^3 + bt^2 + ct + d \in \mathbb{Q}[t]$. Let $\mathrm{Root}_f(\mathbb{C}) = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$. Can we express all these in terms of radicals? Again the answer is yes, but the procedure is much more complicated.

We can perform a similar change of variable to assume $a = 0$. So $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$.

This time, define

$$\begin{aligned}\beta &= \alpha_1 + \alpha_2\\ \gamma &= \alpha_1 + \alpha_3\\ \lambda &= \alpha_1 + \alpha_4\end{aligned}$$

Doing some calculations, we see that

$$\begin{aligned}\beta^2 &= -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)\\ \gamma^2 &= -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)\\ \lambda^2 &= -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)\end{aligned}$$

Now consider

$$\begin{aligned}g &= (t - \beta^2)(t - \gamma^2)(t - \lambda^2)\\ &= t^3 + 2bt^2 + (b^2 - 4d)t - c^2\end{aligned}$$

This we know how to solve, and so we are done.

Quintics and above

So far so good. But how about polynomials of higher degrees? In general, let $f \in \mathbb{Q}[t]$. Can we write down all the roots of f in terms of radicals? We know that the answer is yes if $\deg f \leq 4$.

Unfortunately, for $\deg f \geq 5$, the answer is no. Of course, this "no" means no *in general*. For example, $f = (t-1)(t-2)\cdots(t-5) \in \mathbb{Q}[t]$ has the obvious roots in terms of radicals.

There isn't an easy proof of this result. The general idea is to first associate a *field extension* $F \supseteq \mathbb{Q}$ for our polynomial f. This field F will be obtained by adding all roots of f. Then we associate a *Galois group* G to this field extension. We will then prove a theorem that says f has a solution in terms of radicals if and only if the Galois group is "soluble", where "soluble" has a specific algebraic definition in group theory we will explore later. Finally, we find specific polynomials whose Galois group is not soluble.

2 Field extensions

After all that (hopefully) fun introduction and motivation, we will now start Galois theory in a more abstract way. The modern approach is to describe these in terms of field extensions.

2.1 Field extensions

Definition (Field extension)**.** A *field extension* is an inclusion of a field $K \subseteq L$, where K inherits the algebraic operations from L. We also write this as L/K. Alternatively, we can define this by a injective homomorphism $K \to L$. We say L is an *extension* of K, and K is a *subfield* of L.

Example.

(i) $\mathbb{R}/\mathbb{Q}$ is a field extension.

(ii) $\mathbb{C}/\mathbb{Q}$ is a field extension.

(iii) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ is a field extension over $\mathbb{Q}$.

Given a field extension L/K, we want to quantify how much "bigger" L is compared to K. For example, to get from $\mathbb{Q}$ to $\mathbb{R}$, we need to add a lot of elements (since $\mathbb{Q}$ is countable and $\mathbb{R}$ is uncountable). On the other hand, to get from $\mathbb{R}$ to $\mathbb{C}$, we just need to add a single element $\sqrt{-1}$.

To do so, we can consider L as a vector space over K. We know that L already comes with an additive abelian group structure, and we can define scalar multiplication by simply multiplying: if $a \in K, \alpha \in L$, then $a \cdot \alpha$ is defined as multiplication in L.

Definition (Degree of field extension)**.** The *degree* of L over K is $[L : K]$ is the dimension of L as a vector space over K. The extension is *finite* if the degree is finite.

In this course, we are mostly concerned with finite extensions.

Example.

(i) Consider $\mathbb{C}/\mathbb{R}$. This is a finite extension with degree $[\mathbb{C} : \mathbb{R}] = 2$ since we have a basis of $\{1, i\}$.

(ii) The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ has degree 2 since we have a basis of $\{1, \sqrt{2}\}$.

(iii) The extension $\mathbb{R}/\mathbb{Q}$ is not finite.

We are going to use the following result a lot:

Theorem (Tower Law)**.** Let $F/L/K$ be field extensions. Then

$$[F : K] = [F : L][L : K]$$

Proof. Assume $[F : L]$ and $[L : K]$ are finite. Let $\{\alpha_1, \cdots, \alpha_m\}$ be a basis for L over K, and $\{\beta_1, \cdots, \beta_n\}$ be a basis for F over L. Pick $\gamma \in F$. Then we can write

$$\gamma = \sum_i b_i \beta_i, \quad b_i \in L.$$

For each b_i, we can write as

$$b_i = \sum_j a_{ij}\alpha_j, \quad a_{ij} \in K.$$

So we can write

$$\gamma = \sum_i \left(\sum_j a_{ij}\alpha_j\right)\beta_i = \sum_{i,j} a_{ij}\alpha_j\beta_i.$$

So $T = \{\alpha_j\beta_i\}_{i,j}$ spans F over K. To show that this is a basis, we have to show that they are linearly independent. Consider the case where $\gamma = 0$. Then we must have $b_i = 0$ since $\{\beta_i\}$ is a basis of F over L. Hence each $a_{ij} = 0$ since $\{\alpha_j\}$ is a basis of L over K.

This implies that T is a basis of F over K. So

$$[F : K] = |T| = nm = [F : L][L : K].$$

Finally, if $[F : L] = \infty$ or $[L : K] = \infty$, then clearly $[F : K] = \infty$ as well. So equality holds as well. □

Recall that in IA Numbers and Sets, we defined a real number x to be algebraic if it is a root of some polynomial in integer (or rational) coefficients. We can do this for general field (extensions) as well.

Definition (Algebraic number)**.** Let L/K be a field extension, $\alpha \in L$. We define

$$I_\alpha = \{f \in K[t] : f(\alpha) = 0\} \subseteq K[t]$$

This is the set of polynomials for which α is a root. It is easy to show that I_α is an ideal, since it is the kernel of the ring homomorphism $K[t] \to L$ by $g \mapsto g(\alpha)$.

We say α is *algebraic* over K if $I_\alpha \neq 0$. Otherwise, α is *transcendental* over K.

We say L is *algebraic* over K if every element of L is algebraic.

Example.

(i) $\sqrt[9]{7}$ is algebraic over $\mathbb{Q}$ because $f(\sqrt[9]{7}) = 0$, where $f = t^9 - 7$. In general, any number written with radicals is algebraic over $\mathbb{Q}$.

(ii) π is not algebraic over $\mathbb{Q}$.

These are rather simple examples, and the following lemma will provide us a way of generating much more examples.

Lemma. Let L/K be a finite extension. Then L is algebraic over K.

Proof. Let $n = [L : K]$, and let $\alpha \in L$. Then $1, \alpha, \alpha^2, \cdots, \alpha^n$ are linearly dependent over K (since there are $n + 1$ elements). So there exists some $a_i \in K$ (not all zero) such that

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

So we have a non-trivial polynomial that vanishes at α. So α is algebraic over K.

Since α was arbitrary, L itself is algebraic. □

If L/K is a field extension and $\alpha \in L$ is algebraic, then by definition, there is some polynomial f such that $f(\alpha) = 0$. It is a natural question to ask if there is a "smallest" polynomial that does this job. Obviously we can find a polynomial of smallest *degree* (by the well-ordering principle of the natural numbers), but we can get something even stronger.

Since K is a field, $K[t]$ is a PID (principal ideal domain). This, by definition, implies we can find some (monic) $P_\alpha \in K[t]$ such that $I_\alpha = \langle P_\alpha \rangle$. In other words, every element of I_α is just a multiple of P_α.

Definition (Minimal polynomial)**.** Let L/K be a field extension, $\alpha \in L$. The *minimal polynomial* of α over K is a monic polynomial P_α such that $I_\alpha = \langle P_\alpha \rangle$.

Example.

(i) Consider $\mathbb{R}/\mathbb{Q}$, $\alpha = \sqrt[3]{2}$. Then the minimal polynomial is $P_\alpha = t^3 - 2$.

(ii) Consider $\mathbb{C}/\mathbb{R}$, $\alpha = \sqrt[3]{2}$. Then the minimal polynomial is $P_\alpha = t - \sqrt[3]{2}$.

It should be intuitively obvious that by virtue of being "minimal", the minimal polynomial is irreducible.

Proposition. Let L/K be a field extension, $\alpha \in L$ algebraic over K, and P_α the minimal polynomial. Then P_α is irreducible in $K[t]$.

Proof. Assume that $P_\alpha = QR$ in $K[t]$. So $0 = P_\alpha(\alpha) = Q(\alpha)R(\alpha)$. So $Q(\alpha) = 0$ or $R(\alpha) = 0$. Say $Q(\alpha) = 0$. So $Q \in I_\alpha$. So Q is a multiple of P_α. However, we also know that P_α is a multiple of Q_α. This is possible only if R is a unit in $K[t]$, i.e. $R \in K$. So P_α is irreducible. □

It should also be clear that if f is irreducible and $f(\alpha) = 0$, then f is the minimal polynomial. Often, it is the irreducibility of P_α that is important.

Apart from the minimal polynomial, we can also ask for the minimal field containing α.

Definition (Field generated by α)**.** Let L/K be a field extension, $\alpha \in L$. We define $K(\alpha)$ to be the smallest subfield of L containing K and α. We call $K(\alpha)$ the *field generated by α over K*.

This definition by itself is rather abstract and not very helpful. Intuitively, $K(\alpha)$ is what we get when we add α to K, plus all the extra elements needed to make $K(\alpha)$ a field (i.e. closed under addition, multiplication and inverse). We can express this idea more formally by the following result:

Theorem. Let L/K a field extension, $\alpha \in L$ algebraic. Then

(i) $K(\alpha)$ is the image of the (ring) homomorphism $\phi : K[t] \to L$ defined by $f \mapsto f(\alpha)$.

(ii) $[K(\alpha) : K] = \deg P_\alpha$, where P_α is the minimal polynomial of α over K.

Note that the kernel of the homomorphism ϕ is (almost) by definition the ideal $\langle P_\alpha \rangle$. So this theorem tells us

$$\frac{K[t]}{\langle P_\alpha \rangle} \cong K(\alpha).$$

Proof.

(i) Let F be the image of ϕ. The first step is to show that F is indeed a field. Since F is the image of a ring homomorphism, we know F is a subring of L. Given $\beta \in F$ non-zero, we have to find an inverse.

By definition, $\beta = f(\alpha)$ for some $f \in K[t]$. The idea is to use Bézout's identity. Since $\beta \neq 0$, $f(\alpha) \neq 0$. So $f \notin I_\alpha = \langle P_\alpha \rangle$. So $P_\alpha \nmid f$ in $K[t]$. Since P_α is irreducible, P_α and f are coprime. Then there exists some $g, h \in K[t]$ such that $fg + hP_\alpha = 1$. So $f(\alpha)g(\alpha) = f(\alpha)g(\alpha) + h(\alpha)P_\alpha(\alpha) = 1$. So $\beta g(\alpha) = 1$. So β has an inverse. So F is a field.

From the definition of F, we have $K \subseteq F$ and $\alpha \in F$, using the constant polynomials $f = c \in K$ and the identity $f = t$.

Now, if $K \subseteq G \subseteq L$ and $\alpha \in G$, then G contains all the polynomial expressions of α. Hence $F \subseteq G$. So $K(\alpha) = F$.

(ii) Let $n = \deg P_\alpha$. We show that $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ is a basis for $K(\alpha)$ over K.

First note that since $\deg P_\alpha = n$, we can write

$$\alpha^n = \sum_{i=0}^{n-1} a_i \alpha^i.$$

So any other higher powers are also linear combinations of the α^is (by induction). This means that $K(\alpha)$ is spanned by $1, \cdots, \alpha^{n-1}$ as a K vector space.

It remains to show that $\{1, \cdots, \alpha^{n-1}\}$ is linearly independent. Assume not. Then for some b_i, we have

$$\sum_{i=0}^{n-1} b_i \alpha^i = 0.$$

Let $f = \sum b_i t^i$. Then $f(\alpha) = 0$. So $f \in I_\alpha = \langle P_\alpha \rangle$. However, $\deg f < \deg P_\alpha$. So we must have $f = 0$. So all $b_i = 0$. So $\{1, \cdots, \alpha^{n-1}\}$ is a basis for $K(\alpha)$ over K. So $[K(\alpha) : K] = n$. □

Corollary. Let L/K be a field extension, $\alpha \in L$. Then α is algebraic over K if and only if $K(\alpha)/K$ is a finite extension.

Proof. If α is algebraic, then $[K(\alpha) : K] = \deg P_\alpha < \infty$ by above. So the extension is finite.

If $K \subseteq K(\alpha)$ is a finite extension, then by previous lemma, the entire $K(\alpha)$ is algebraic over K. So α is algebraic over K. □

We can extend this definition to allow more elements in the generating set.

Definition (Field generated by elements)**.** Let L/K be a field extension, $\alpha_1, \cdots, \alpha_n \subseteq L$. We define $K(\alpha_1, \cdots, \alpha_n)$ to be the smallest subfield of L containing K and $\alpha_1, \cdots, \alpha_n$.

We call $K(\alpha_1, \cdots, \alpha_n)$ the *field generated by* $\alpha_1, \cdots, \alpha_n$ over K.

And we can prove some similar results.

Theorem. Suppose that L/K is a field extension.

(i) If $\alpha_1, \cdots, \alpha_n \in L$ are algebraic over K, then $K(\alpha_1, \cdots, \alpha_n)/K$ is a finite extension.

(ii) If we have field extensions $L/F/K$ and F/K is a finite extension, then $F = K(\alpha_1, \cdots, \alpha_n)$ for some $\alpha_1, \cdots, \alpha_n \in L$.

Proof.

(i) We prove this by induction. Since α_1 is algebraic over K, $K \subseteq K(\alpha_1)$ is a finite extension.

For $1 \leq i < n$, α_{i+1} is algebraic over K. So α_{i+1} is also algebraic over $K(\alpha_1, \cdots, \alpha_i)$. So $K(\alpha_1, \cdots, \alpha_i) \subseteq K(\alpha_1, \cdots, \alpha_i)(\alpha_{i+1})$ is a finite extension. But $K(\alpha_1, \cdots, \alpha_i)(\alpha_{i+1}) = K(\alpha_1, \cdots, \alpha_{i+1})$. By the tower law, $K \subseteq K(\alpha_i, \cdots, \alpha_{i+1})$ is a finite extension.

(ii) Since F is a finite dimensional vector space over K, we can take a basis $\{\alpha_1, \cdots, \alpha_n\}$ of F over K. Then it should be clear that $F = K(\alpha_1, \cdots, \alpha_n)$. □

When studying polynomials, the following result from IB Groups, Rings and Modules is often helpful:

Proposition (Eisenstein's criterion)**.** Let $f = a_n t^n + \cdots + a_1 t + a_0 \in \mathbb{Z}[t]$. Assume that there is some prime number p such that

(i) $p \mid a_i$ for all $i < n$.

(ii) $p \nmid a_n$

(iii) $p^2 \nmid a_0$.

Then f is irreducible in $\mathbb{Q}[t]$.

Example. Consider the field extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \subseteq \mathbb{R},$$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \subseteq \mathbb{R}.$$

We have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ since $\{1, \sqrt{2}\}$ is a basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

How about $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$? By the Eisenstein criterion, we know that $t^3 - 2$ is irreducible in $\mathbb{Q}[t]$. So the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $t^3 - 2$ which has degree 3. So $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

These results immediately tells that $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$. Otherwise, this entails that $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt{2})$. Then the tower law says that

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

In particular, plugging the numbers in entails that that 3 is a factor of 2, which is clearly nonsense. Similarly, $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$.

How about the inclusion $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$? We now show that the minimal polynomial $P_{\sqrt[3]{2}}$ of $\sqrt[3]{2}$ over $\mathbb{Q}(\sqrt{2})$ is $t^3 - 2$.

Suppose not. Then $t^3 - 2$ is reducible, with the real $P_{\sqrt[3]{2}}$ as one of its factors. Let $t^3 - 2 = P_{\sqrt[3]{2}} \cdot R$ for some non-unit polynomial R.

We know that $P_{\sqrt[3]{2}}$ does not have degree 3 (or else it would be $t^3 - 2$), and not degree 1, since a degree 1 polynomial has a root. So it has degree 2. So R has degree 1. Then R has a root, i.e. $R(\beta) = 0$ for some $\beta \in \mathbb{Q}(\sqrt{2})$. So $\beta^3 - 2 = 0$. Hence $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$. Again, by the tower law, we have

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}].$$

Again, this is nonsense since it entails that 3 is a factor of 2. So the minimal polynomial is indeed $t^3 - 2$. So $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$ by the tower law.

Alternatively, we can obtain this result by noting that the tower law on $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ and $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ entails that 2 and 3 are both factors of $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$. So it is at least 6. Then since $t^3 - 2 \in \mathbb{Q}(\sqrt{2})[t]$ has $\sqrt[3]{2}$ as a root, the degree is at most 6. So it is indeed 6.

2.2 Ruler and compass constructions

Before we develop our theory further, we first look into a rather unexpected application of field extensions. We are going to look at some classic problems in geometry, and solve them using what we've learnt so far. In particular, we want to show that certain things cannot be constructed using a compass and a ruler (as usual, we assume the ruler does not have markings on it).

It is often easy to prove that certain things are constructible — just exhibit an explicit construction of it. However, it is much more difficult to show that things are *not* constructible. Two classical examples are

(i) Doubling the cube: Given a cube, can we construct the side of another cube whose volume is double the volume of the original cube?

(ii) Trisecting an angle: Given an angle, can we divide the angle into three equal angles?

The idea here is to associate with each possible construction a field extension, and then prove certain results about how these field extensions should behave. We then show that if we could, say, double the cube, then this construction would inevitable break some of the properties it should have.

Firstly, we want to formulate our problem in a more convenient way. In particular, we will view the plane as $\mathbb{R}^2$, and describe lines and circles by equations. We also want to describe "compass and ruler" constructions in a more solid way.

Definition (Constructible points)**.** Let $S \subseteq \mathbb{R}^2$ be a set of (usually finite) points in the plane.

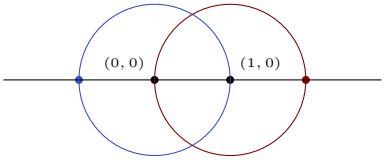
A "ruler" allows us to do the following: if $P, Q \in S$, then we can draw the line passing through P and Q.

A "compass" allows us to do the following: if $P, Q, Q' \in S$, then we can draw the circle with center at P and radius of length QQ'.

Any point $R \in \mathbb{R}^2$ is *1-step constructible* from S if R belongs to the intersection of two distinct lines or circles constructed from S using rulers and compasses.

A point $R \in \mathbb{R}^2$ is *constructible* from S if there is some $R_1, \cdots, R_n = R \in \mathbb{R}^2$ such that R_{i+1} is 1-step constructible from $S \cup \{R_1, \cdots, R_i\}$ for each i.

Example. Let $S = \{(0,0),(1,0)\}$. What can we construct? It should be easy to see that $(n,0)$ for all $n \in \mathbb{Z}$ are all constructible from S. In fact, we can show that all points of the form $(m,n) \in \mathbb{Z}$ are constructible from S.



Definition (Field of S)**.** Let $S \subseteq \mathbb{R}^2$ be finite. Define the *field of* S by

$$\mathbb{Q}(S) = \mathbb{Q}(\{\text{coordinates of points in } S\}) \subseteq \mathbb{R},$$

where we put in the x coordinate and y coordinate separately into the generating set.

For example, if $S = \{(\sqrt{2}, \sqrt{3})\}$, then $\mathbb{Q}(S) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
The key theorem we will use to prove our results is

Theorem. Let $S \subseteq \mathbb{R}^2$ be finite. Then

(i) If R is 1-step constructible from S, then $[\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)] = 1$ or 2.

(ii) If $T \subseteq \mathbb{R}^2$ is finite, $S \subseteq T$, and the points in T are constructible from S, Then $[\mathbb{Q}(S \cup T) : \mathbb{Q}(S)] = 2^k$ for some k (where k can be 0).

Proof. By assumption, there are distinct lines or circles C, C' constructed from S using ruler and compass, such that $R \in C \cap C'$. By elementary geometry, C and C' can be given by the equations

$$C : a(x^2 + y^2) + bx + cy + d = 0,$$
$$C' : a'(x^2 + y^2) + b'x + c'y + d' = 0.$$

where $a, b, c, d, a', b', c', d' \in \mathbb{Q}(S)$. In particular, if we have a line, then we can take $a = 0$.

Let $R = (r_1, r_2)$. If $a = a' = 0$ (i.e. C and C' are lines), then solving the two linear equations gives $r_1, r_2 \in \mathbb{Q}(S)$. So $[\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)] = 1$.

So we can now assume wlog that $a \neq 0$. We let

$$p = a'b - ab', \quad q = a'c - ac', \quad \ell = a'd - ad',$$

which are the coefficients when we perform $a' \times C - a \times C'$. Then by assumption, $p \neq 0$ or $q \neq 0$. Otherwise, c and c' would be the same curve. wlog $p \neq 0$. Then since (r_1, r_2) satisfy both equations of C and C', they satisfy

$$px + qy + \ell = 0.$$

In other words, $pr_1 + qr_2 + \ell = 0$. This tells us that

$$r_1 = -\frac{qr_2 + \ell}{p}. \tag{$*$}$$

If we put r_1, r_2 into the equations of C and C' and use $(*)$, we get an equation of the form

$$\alpha r_2^2 + \beta r_2 + \gamma = 0,$$

where $\alpha, \beta, \gamma \in \mathbb{Q}(S)$. So we can find r_2 (and hence r_1 using linear relations) using only a single radical of degree 2. So

$$[\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)] = [\mathbb{Q}(S)(r_2) : \mathbb{Q}(S)] = 1 \text{ or } 2,$$

since the minimal polynomial of r_2 over $\mathbb{Q}(S)$ has degree 1 or 2.

Then (ii) follows directly from induction, using the tower law. □

Corollary. It is impossible to "double the cube".

Proof. Consider the cube with unit side length, i.e. we are given the set $S = \{(0,0),(1,0)\}$. Then doubling the cube would correspond to constructing a side of length ℓ such that $\ell^3 = 2$, i.e. $\ell = \sqrt[3]{2}$. Thus we need to construct a point $R = (\sqrt[3]{2}, 0)$ from S.

If we can indeed construct this R, then we need

$$[\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)] = 2^k$$

for some k. But we know that $\mathbb{Q}(S) = \mathbb{Q}$ and $\mathbb{Q}(S \cup \{R\}) = \mathbb{Q}(\sqrt[3]{2})$, and that

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

This is a contradiction since 3 is not a power of 2. □

2.3 K-homomorphisms and the Galois Group

Usually in mathematics, we not only want to study objects, but maps between objects. Suppose we have two field extensions $K \subseteq L$ and $K \subseteq L'$. What should a map between these two objects look like? Obviously, we would like this map to be a field homomorphisms between L and L'. Moreover, since this is a map between the two field *extensions*, and not just the fields themselves, we would like this map to preserve things in K, and is just a map between the "extended parts" of L and L'.

Definition (K-homomorphism)**.** Let L/K and L'/K be field extensions. A *K-homomorphism* $\phi : L \to L'$ is a ring homomorphism such that $\phi|_K = \mathrm{id}$, i.e. it fixes everything in K. We write $\mathrm{Hom}_K(L, L')$ for the set of all K-homomorphisms $L \to L'$.

A *K-isomorphism* is a K-homomorphism which is an isomorphism of rings. A *K-automorphism* is a K-isomorphism $L \to L$. We write $\mathrm{Aut}_K(L)$ for the set of all K-automorphism $L \to L$.

There are a couple of things to take note of

(i) Given any $\phi \in \mathrm{Hom}_K(L, L')$, we know that

  (a) Since $\phi|_K = \mathrm{id}$, we know that $\ker \phi \neq L$. Since we know that $\ker \phi$ is an ideal, and a field only has two ideals, we must have $\ker \phi = 0$. So ϕ is injective. It is, in fact, true that any homomorphisms of fields is injective.

  (b) ϕ gives an isomorphism $L \to \phi(L)$. So $\phi(L)$ is a field and we get the field extensions $K \subseteq \phi(L) \subseteq L'$.

(ii) If $[L : K] = [L' : K] < \infty$, then any homomorphism in $\mathrm{Hom}_K(L, L')$ is in fact an isomorphism. So

$$\{K\text{-homomorphisms} : L \to L'\} = \{K\text{-isomorphisms} : L \to L'\},$$

This is since any K-homomorphism $\phi : L \to L'$ is an injection. So $[L : K] = [\phi(L) : K]$. Hence we know that $[L' : K] = [\phi(L) : K]$. But we know that $\phi(L)$ is a subfield of L'. This is possible only if $L' = \phi(L)$. So ϕ is a surjection, and hence an isomorphism.

In particular, $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L, L)$.

Example. We want to determine $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$. If we pick any $\psi \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$, then

$$(\psi(\sqrt{-1}))^2 + 1 = \psi(\sqrt{-1}^2 + 1) = \psi(0) = 0.$$

So under any automorphism ψ, the image of $\sqrt{-1}$ is a root of $t^2 + 1$. Therefore $\psi(\sqrt{-1}) = \sqrt{-1}$ or $-\sqrt{-1}$. In the first case, ψ is the identity. In the second case, the automorphism is $\phi : a + b\sqrt{-1} \mapsto a - b\sqrt{-1}$, i.e. the complex conjugate. So $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}, \phi\}$.

Similarly, we can show that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = \{\mathrm{id}, \phi\}$, where ϕ swaps $\sqrt{2}$ with $-\sqrt{2}$.

Example. Let $\mu^3 = 1$ but $\mu \neq 1$ (i.e. μ is a third root of unity). We want to determine $A = \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{C})$.

First define ϕ, ψ by

$$\phi(\sqrt[3]{2}) = \sqrt[3]{2}\mu$$
$$\psi(\sqrt[3]{2}) = \sqrt[3]{2}\mu^2,$$

We have $\phi, \psi \in A$. Are there more?

Let $\lambda \in A$. Then we must have

$$(\lambda(\sqrt[3]{2}))^3 - 2 = 0.$$

So $\lambda(\sqrt[3]{2})$ is a root of $t^3 - 2$. So it is either $\sqrt[3]{2}$, $\sqrt[3]{2}\mu$ or $\sqrt[3]{2}\mu^2$. So λ is either id, ϕ or ψ. So $A = \{\mathrm{id}, \phi, \psi\}$.

Note that in general, if α is algebraic over $\mathbb{Q}$, then $\mathbb{Q}(\alpha) \cong \mathbb{Q}[t]/\langle P_\alpha \rangle$. Hence to specify a $\mathbb{Q}$-homomorphism from $\mathbb{Q}(\alpha)$, it suffices to specify the image of t, or just the image of α.

We will later see that the number of automorphisms $|\mathrm{Aut}_K(L)|$ is bounded above by the degree of the extension $[L : K]$. However, we need not always have $[L : K]$ many automorphisms. When we *do* have enough automorphisms, we call it a *Galois extension*.

Definition (Galois extension)**.** Let L/K be a finite field extension. This is a *Galois extension* if $|\mathrm{Aut}_K(L)| = [L : K]$.

Definition (Galois group)**.** The *Galois group* of a Galois extension L/K is defined as $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$. The group operation is defined by function composition. It is easy to see that this is indeed a group.

Example. The extension $\mathbb{Q}(\sqrt{7})/\mathbb{Q}$ is Galois. The degree $[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2$, and the automorphism group is $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{7})) = \{\mathrm{id}, \phi\}$, where ϕ swaps $\sqrt{7}$ with $-\sqrt{7}$.

Example. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois. The degree is $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, but the automorphism group is $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{\mathrm{id}\}$.

To show that there is no other automorphism, note that the automorphism group can be viewed as a subset of $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{C})$. We have just seen that $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{C})$ has three elements, but only the identity maps $\mathbb{Q}(\sqrt[3]{2})$ to itself, while the others map $\sqrt[3]{2}$ to $\sqrt[3]{2}\mu^i \notin \mathbb{Q}(\sqrt[3]{2})$. So this is the only automorphism.

The way we should think about this is that there is something missing in $\mathbb{Q}(\sqrt[3]{2})$, namely μ. Without the μ, we cannot get the other automorphisms we need. In fact, in the next example, we will show that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, \mu)$ is Galois.

Example. $\mathbb{Q}(\sqrt[3]{2}, \mu)/\mathbb{Q}$ is a Galois extension. Firstly, we know that $[\mathbb{Q}(\sqrt[3]{2}, \mu) : \mathbb{Q}(\sqrt[3]{2})] = 2$ because $\mu^3 - 1 = 0$ implies $\mu^2 + \mu + 1 = 0$. So the minimal polynomial has degree 2. This also means that $\mu \notin \mathbb{Q}(\sqrt[3]{2})$. We also know that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. So we have

$$[\mathbb{Q}(\sqrt[3]{2}, \mu) : \mathbb{Q}] = 6$$

by the Tower law.

Now denote $\alpha = \sqrt[3]{2}$, $\beta = \sqrt[3]{2}\mu$ and $\gamma = \sqrt[3]{2}\mu^2$. Then $\mathbb{Q}(\sqrt[3]{2}, \mu) = \mathbb{Q}(\alpha, \beta, \gamma)$. Now let $\phi \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \mu))$, then $\phi(\alpha)$, $\phi(\beta)$ and $\phi(\gamma)$ are roots of $t^3 - 2$. These roots are exactly α, β, γ. So

$$\{\phi(\alpha), \phi(\beta), \phi(\gamma)\} = \{\alpha, \beta, \gamma\}.$$

Hence ϕ is completely determined by a permutation of the roots of $t^3 - 2$. So $\mathrm{Aut}_{\mathbb{Q}}(\sqrt[3]{2}, \mu) \cong S_3$ and $|\mathrm{Aut}_{\mathbb{Q}}(\sqrt[3]{2}, \mu)| = 6$.

Most of the time, we will only be interested in Galois extensions. The main reason is that Galois extensions satisfy the *fundamental theorem of Galois theory*, which roughly says: if L/K is a finite Galois extension, then there is a one-to-one correspondence of the set of subgroups $H \leq \mathrm{Gal}(L/K)$ and the intermediate fields $K \subseteq F \subseteq L$. In particular, the normal subgroups corresponds to the "normal extensions", which is something we will define later.

However, just as we have seen, it is not straightforward to check if an extension is Galois, even in specific cases like the examples above. Fortunately, by the time we reach the proper statement of the fundamental theorem, we would have developed enough machinery to decide easily whether certain extensions are Galois.

2.4 Splitting fields

As mentioned in the introduction, one major motivation for Galois theory is to study the roots of polynomials. So far, we have just been talking about field extensions. The idea here is given a field K and a polynomial $f \in K[t]$, we would like to study the field extension obtained by adding all roots of f. This is known as the *splitting field* of f (over K).

Notation. Let L/K be a field extension, $f \in K[t]$. We write $\mathrm{Root}_f(L)$ for the roots of f in L.

First, we establish a correspondence between the roots of a polynomial and K-homomorphisms.

Lemma. Let L/K be a field extension, $f \in K[t]$ irreducible, $\deg f > 0$. Then there is a 1-to-1 correspondence

$$\mathrm{Root}_f(L) \longleftrightarrow \mathrm{Hom}_K(K[t]/\langle f\rangle, L).$$

Proof. Since f is irreducible, $\langle f\rangle$ is a maximal ideal. So $K[t]/\langle f\rangle$ is a field. Also, there is a natural inclusion $K \hookrightarrow K[t]/\langle f\rangle$. So it makes sense to talk about $\mathrm{Hom}_K(K[t]/\langle f\rangle, L)$.

To any $\beta \in \mathrm{Root}_f(L)$, we assign $\phi : K[t]/\langle f\rangle \to L$ where we map $\bar{t} \mapsto \beta$ ($\bar{t}$ is the equivalence class of t). This is well defined since if $\bar{t} = \bar{g}$, then $g = t + hf$ for some $h \in K[t]$. So $\phi(\bar{g}) = \phi(\overline{t + hf}) = \beta + h(\beta)f(\beta) = \beta$.

Conversely, given any K-homomorphism $\phi : K[t]/\langle f\rangle \to L$, we assign $\beta = \phi(\bar{t})$. This is a root since $f(\beta) = f(\phi(\bar{t})) = \phi(f(\bar{t})) = \phi(0) = 0$.

This assignments are inverses to each other. So we get a one-to-one correspondence. □

Recall that if $K \subseteq F$ is a field extension, then for any $\alpha \in F$ with minimal polynomial P_α, we have $K[t]/\langle P_\alpha\rangle \cong K(\alpha)$. Since an irreducible f is the minimal polynomial of its roots, we can view the above lemma as telling us something about $\mathrm{Hom}_K(K(\alpha), L)$.

Corollary. Let L/K be a field extension, $f \in K[t]$ irreducible, $\deg f > 0$. Then

$$|\mathrm{Hom}_K(K[t]/\langle f\rangle, L)| \leq \deg f.$$

In particular, if $E = K[t]/\langle f\rangle$, then

$$|\operatorname{Aut}_K(E)| = |\operatorname{Root}_f(E)| \leq \deg f = [E : K].$$

So E/K is a Galois extension iff $|\operatorname{Root}_f(E)| = \deg f$.

Proof. This follows directly from the following three facts:

- $|\operatorname{Root}_f(L)| \leq \deg f$
- $\operatorname{Aut}_K(E) = \mathrm{Hom}_K(E, E)$
- $\deg f = [K(\alpha) : K] = [E : K]$. □

Definition (Splitting field)**.** Let L/K be a field extensions, $f \in K[t]$. We say f *splits* over L if we can factor f as

$$f = a(t - \alpha_1)\cdots(t - \alpha_n)$$

for some $a \in K$ and $\alpha_j \in L$. Alternatively, this says that L contains all roots of f.

We say L is a *splitting field* of f if $L = K(\alpha_1, \cdots, \alpha_n)$. This is the smallest field where f has all its roots.

Example.

- $\mathbb{C}$ is the splitting field of $t^2 + 1 \in \mathbb{R}[t]$.

– $\mathbb{Q}(\sqrt[3]{2}, \mu)$ is a splitting field of $t^3 - 2 \in \mathbb{Q}[t]$, where μ is a third root of unity.

– By the fundamental theorem of algebra, for any $K \subseteq \mathbb{C}$ and $f \in K[t]$, there is a splitting field $L \subseteq \mathbb{C}$ of f.

Note that the degree of the splitting field need not be (bounded by) the degree of the polynomial. In the second example, we have $[\mathbb{Q}(\sqrt[3]{2}, \mu) : \mathbb{Q}] = 6$, but $t^3 - 2$ only has degree 3.

More generally, we can show that every polynomial has a splitting field, and this is unique up to isomorphism. This is important, since we would like to talk about *the* splitting field of a polynomial all the time.

Theorem. Let K be a field, $f \in K[t]$. Then

(i) There is a splitting field of f.

(ii) The splitting field is unique (up to K-isomorphism).

Proof.

(i) If $\deg f = 0$, then K is a splitting field of f. Otherwise, we add the roots of f one by one.

Pick $g \mid f$ in $K[t]$, where g is irreducible and $\deg g > 0$. We have the field extension $K \subseteq K[t]/\langle g\rangle$. Let $\alpha_1 = \bar{t}$. Then $g(\alpha_1) = 0$ which implies that $f(\alpha_1) = 0$. Hence we can write $f = (t - \alpha_1)h$ in $K(\alpha_1)[t]$. Note that $\deg h < \deg f$. So we can repeat the process on h iteratively to get a field extensions $K \subseteq K(\alpha_1, \cdots, \alpha_n)$. This $K(\alpha_1, \cdots, \alpha_n)$ is a splitting field of f.

(ii) Assume L and L' are both splitting fields of f over K. We want to find a K-isomorphism from L to L'.

Pick largest F, F' such that $K \subseteq F \subseteq L$ and $K \subseteq F' \subseteq L'$ are field extensions and there is a K-isomorphism from $\psi : F \to F'$. By "largest", we mean we want to maximize $[F : K]$.

We want to show that we must have $F = L$. Then we are done because this means that F' is a splitting field, and hence $F' = L'$.

So suppose $F \neq L$. We will try to produce a larger $\tilde{F}$ with K-isomorphism $\tilde{F} \to \tilde{F}' \subseteq L'$.

Since $F \neq L$, we know that there is some $\alpha \in \mathrm{Root}_f(L)$ such that $\alpha \notin F$. Then there is some irreducible $g \in K[t]$ with $\deg g > 0$ such that $g(\alpha) = 0$ and $g \mid f$. Say $f = gh$.

Now we know there is an isomorphism $F[t]/\langle g\rangle \to F(\alpha)$ by $\bar{t} \mapsto \alpha$. The isomorphism $\psi : F \to F'$ extends to a isomorphism $\mu : F[t] \to F'[t]$. Then since the coefficients of f are in K, we have $f = \mu(f) = \mu(g)\mu(h)$. So $\mu(g) \mid f$ in $F'[t]$. Since g is irreducible in $F[t]$, $\mu(g)$ is irreducible in $F'[t]$. So there is some $\alpha' \in \mathrm{Root}_{\mu(g)}(L') \subseteq \mathrm{Root}_f(L')$ and isomorphism $F'[t]/\langle\mu(g)\rangle \to F'(\alpha')$.

Now μ induces a K-isomorphism $F[t]/\langle g\rangle \to F'[t]/\langle\mu(g)\rangle$, which in turn induces a K-isomorphism $F(\alpha) \to F'(\alpha')$. This contradicts the maximality of F. So we must have had $F = L$. □

Note that the splitting is unique just up to isomorphism. We could be quotienting by different polynomials and still get the same splitting field.

Example. $\mathbb{Q}(\sqrt{7})$ is a splitting field of $t^2 - 7 \in \mathbb{Q}[t]$. At the same time, $\mathbb{Q}(\sqrt{7})$ is also a splitting field of $t^2 + 3t + \frac{1}{2} \in \mathbb{Q}[t]$.

2.5 Algebraic closures

The splitting field gives us the field with the root of one particular polynomial. We could be greedy and ask for the roots for *all* polynomials, and get the *algebraic closure*. The algebraic closure will not be of much use in this course, but is a nice thing to know about. The major theorems would be the existence and uniqueness of algebraic closures.

Definition (Algebraically closed field)**.** A field L is *algebraically closed* if for all $f \in L[t]$, we have

$$f = a(t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_n)$$

for some $a, \alpha_i \in L$. In other words, L contains all roots of its polynomials.

Let L/K be a field extension. We say L is an algebraic closure of K if

- L is algebraic over K
- L is algebraically closed.

Example. L is an algebraically closed field iff ($L \subseteq E$ is a finite extension implies $E = L$).

This is since if $L \subseteq E$ is finite, then E is algebraic over L, and hence must be L.

Example. $\mathbb{C}$ is algebraically closed by the fundamental theorem of algebra, and is the algebraic closure of $\mathbb{R}$ (but not $\mathbb{Q}$).

Before we prove our next theorem, we need the following technical lemma:

Lemma. If R is a commutative ring, then it has a maximal ideal. In particular, if I is an ideal of R, then there is a maximal ideal that contains I.

Proof. Let

$$\mathcal{P} = \{I : I \text{ is an ideal of } R, I \neq R\}.$$

If $I_1 \subseteq I_2 \subseteq \cdots$ is any chain of $I_i \in P$, then $I = \bigcup I_i \in \mathcal{P}$. By Zorn's lemma, there is a maximal element of $\mathcal{P}$ (containing I). So R has at least one maximal ideal (containing I). □

Theorem (Existence of algebraic closure)**.** Any field K has an algebraic closure.

Proof. Let

$$\mathcal{A} = \{\lambda = (f, j) : f \in K[t] \text{ irreducible monic}, 1 \leq j \leq \deg f\}.$$

We can think of j as labelling which root of f we want. For each $\lambda \in \mathcal{A}$, we assign a variable t_λ. We take

$$R = K[t_\lambda : \lambda \in \mathcal{A}]$$

to be the polynomial ring over K with variables t_λ. This R contains all the "roots" of the polynomials in K. However, we've got a bit too much. For example, (if $K = \mathbb{Q}$), in R, $\sqrt{3}$ and $\sqrt{3}+1$ would be put down as separate, unrelated variables. So we want to quotient this R by something.

For every monic and irreducible $f \in K[t]$, we define

$$\tilde{f} = f - \prod_{j=1}^{\deg f} (t - t_{(f,j)}) \in R[t].$$

If we want the $t_{(f,j)}$ to be roots of f, then $\tilde{f}$ should vanish for all f. Denote the coefficient of t^ℓ in $\tilde{f}$ by $b_{(f,\ell)}$. Then we want $b_{(f,\ell)} = 0$ for all f, ℓ.

To do so, let $I \subseteq R$ be the ideal generated by all such coefficients. We now want to quotient R by I. We first have to check that $I \neq R$.

Suppose not. So there are $b_{(f_1,\ell_1)}, \cdots, b_{(f_r,\ell_r)}$ with $g_1, \cdots, g_r \in R$ such that

$$g_1 b_{(f_1,\ell_1)} + \cdots + g_r b_{(f_r,\ell_r)} = 1. \tag{$*$}$$

We will attempt to reach a contradiction by constructing a homomorphism ϕ that sends each $b_{(f_i,\ell_i)}$ to 0.

Let E be a splitting field of $f_1 f_2 \cdots f_r$. So in $E[t]$, for each i, we can write

$$f_i = \prod_{j=1}^{\deg f_i} (t - \alpha_{i,j}).$$

Then we define a homomorphism $\phi : R \to E$ by

$$\begin{cases} \phi(t_{(f_i,j)}) = \alpha_{i,j} \\ \phi(t_\lambda) = 0 & \text{otherwise} \end{cases}$$

This induces a homomorphism $\tilde{\phi} : R[t] \to E[t]$.

Now apply

$$\begin{aligned} \tilde{\phi}(\tilde{f}_i) &= \tilde{\phi}(f_i) - \prod_{j=1}^{\deg f_i} \tilde{\phi}(t - t_{(f_i,j)}) \\ &= f_i - \prod_{j=1}^{\deg f_i} (t - \alpha_{i,j}) \\ &= 0 \end{aligned}$$

So $\phi(b_{(f_i,\ell_i)}) = 0$ as $b_{(f_i,\ell_i)}$ is a coefficient of f_i.

Now we apply ϕ to $(*)$ to obtain

$$\phi(g_1 b_{(f_1,\ell_1)} + \cdots + g_r b_{(f_r,\ell_r)}) = \phi(1).$$

But this is a contradiction since the left had side is 0 while the right is 1. Hence we must have $I \neq R$.

We would like to quotient by I, but we have to be a bit more careful, since the quotient need not be a field. Instead, pick a maximal ideal M containing I, and consider $L = R/M$. Then L is a field. Moreover, since we couldn't

have quotiented out anything in K (any ideal containing anything in K would automatically contain all of R), this is a field extension L/K. We want to show that L is an algebraic closure.

Now we show that L is algebraic over K. This should all work out smoothly, since that's how we constructed L. First we pick $\alpha \in L$. Since $L = R/M$ and R is generated by the terms t_λ, there is some $(f_1, j_1), \cdots, (f_r, j_r)$ such that

$$\alpha \in K(\bar{t}_{(f_i,j_i)}, \cdots, \bar{t}_{(f_r,j_r)}).$$

So α is algebraic over K if each $\bar{t}_{(f_i,j_i)}$ is algebraic over K. To show this, note that $\tilde{f}_i = 0$, since we've quotiented out each of its coefficients. So by definition,

$$0 = f_i(t) - \prod_{j=1}^{\deg f_i} (t - \bar{t}_{(f_i,j)}).$$

So $f_i(\bar{t}_{(f_i,j_i)}) = 0$. So done.

Finally, we have to show that L is algebraically closed. Suppose $L \subseteq E$ is a finite (and hence algebraic) extension. We want to show that $L = E$.

Consider arbitrary $\beta \in E$. Then β is algebraic over L, say a root of $f \in L[t]$. Since every coefficient of f can be found in some finite extension $K(\bar{t}_{(f_i,j_i)}, \cdots, \bar{t}_{(f_r,j_r)})$, there is a finite extension F of K that contains all coefficients of f. Since $F(\beta)$ is a finite extension of F, we know $F(\beta)$ is a finite and hence algebraic extension of K. In particular, β is algebraic in K.

Let P_β be the minimal polynomial of β over K. Since all polynomials in K split over L by construction ($f(t) = \prod(t - \bar{t}_{(f,j)})$), its roots must in L. In particular, $\beta \in L$. So $L = E$. □

Theorem (Uniqueness of algebraic closure)**.** Any field K has a unique algebraic closure up to K-isomorphism.

This is the same proof as the proof that the splitting field is unique — given two algebraic closures, we take the largest subfield of the algebraic closures that biject with each other. However, since there could be infinitely many subfields, we have to apply Zorn's lemma to obtain the maximal such subfield.

Proof. (sketch) Suppose L, L' are both algebraic closures of K. Let

$$\mathcal{H} = \{(F, \psi) : K \subseteq F \subseteq L, \psi \in \mathrm{Hom}_K(F, L')\}.$$

We define a partial order on $\mathcal{H}$ by $(F_1, \psi_1) \leq (F_2, \psi_2)$ if $F_1 \leq F_2$ and $\psi_1 = \psi_2|_{F_1}$.

We have to show that chains have upper bounds. Given a chain $\{(F_\alpha, \psi_\alpha)\}$, we define

$$F = \bigcup F_\alpha, \quad \psi(x) = \psi_\alpha(x) \text{ for } x \in F_\alpha.$$

Then $(F, \psi) \in \mathcal{H}$. Then applying Zorn's lemma, there is a maximal element of $\mathcal{H}$, say (F, ψ).

Finally, we have to prove that $F = L$, and that $\psi(L) = L'$. Suppose $F \neq L$. Then we attempt to produce a larger $\tilde{F}$ and a K-isomorphism $\tilde{F} \to \tilde{F}' \subseteq L'$. Since $F \neq L$, there is some $\alpha \in L \setminus F$. Since L is an algebraic extension of K, there is some irreducible $g \in K[t]$ such that $\deg g > 0$ and $g(\alpha) = 0$.

Now there is an isomorphism $F[t]/\langle g \rangle \to F(\alpha)$ defined by $\bar{t} \mapsto \alpha$. The isomorphism $\psi : F \to F'$ then extends to an isomorphism $\mu : F[t] \to F'[t]$

and thus to $\mathbb{F}[t]/\langle g\rangle \to F'[t]/\langle \mu(g)\rangle$. Then if α' is a root of $\mu(g)$, then we have $F'[t]//\langle \mu(g)\rangle \cong F'(\alpha')$. So this gives an isomorphism $F(\alpha) \to F(\alpha')$. This contradicts the maximality of ϕ.

By doing the argument the other way round, we must have $\psi(L) = L'$. So done. □

2.6 Separable extensions

Here we will define what it means for an extension to be separable. This is done via defining separable polynomials, and then an extension is separable if all minimal polynomials are separable.

At first, the definition of separability might seem absurd — surely every polynomial should be separable. Indeed, polynomials that are not separable tend to be weird, and our theories often break without separability. Hence it is important to figure out when polynomials are separable, and when they are not. Fortunately, we will end up with a result that tells us exactly when a polynomial is not separable, and this is just a very small, specific class. In particular, in fields of characteristic zero, all polynomials are separable.

Definition (Separable polynomial)**.** Let K be a field, $f \in K[t]$ non-zero, and L a splitting field of f. For an irreducible f, we say it is *separable* if f has no repeated roots, i.e. $|\operatorname{Root}_f(L)| = \deg f$. For a general polynomial f, we say it is *separable* if all its irreducible factors in $K[t]$ are separable.

It should be obvious from definition that if P is separable and $Q \mid P$, then Q is also separable.

Note that some people instead define a separable polynomial to be one with no repeated roots, so $(x-2)^2$ over $\mathbb{Q}$ would not be separable under this definition.

Example. Any linear polynomial $t - a$ (with $a \in K$) is separable.

This is, however, not a very interesting example. To get to more interesting examples, we need even more preparation.

Definition (Formal derivative)**.** Let K be a field, $f \in K[t]$. *(Formal) differentiation* the K-linear map $K[t] \to K[t]$ defined by $t^n \mapsto nt^{n-1}$.

The image of a polynomial f is the *derivative* of f, written f'.

This is similar to how we differentiate real or complex polynomials (in case that isn't obvious).

The following lemma summarizes the properties of the derivative we need.

Lemma. Let K be a field, $f, g \in K[t]$. Then

(i) $(f+g)' = f' + g'$, $(fg)' = fg' + f'g$.

(ii) Assume $f \neq 0$ and L is a splitting field of f. Then f has a repeated root in L if and only if f and f' have a common (non-constant) irreducible factor in $K[t]$ (if and only if f and f' have a common root in L).

This will allow us to show when irreducible polynomials are separable.

Proof.

(i) $(f+g)' = f' + g'$ is true by linearity.

To show that $(fg)' = fg' + f'g$, we use linearity to reduce to the case where $f = t^n, g = t^m$. Then both sides are $(n+m)t^{n+m-1}$. So this holds.

(ii) First assume that f has a repeated root. So let $f = (t-\alpha)^2 h \in L[t]$ where $\alpha \in L$. Then $f' = 2(t-\alpha)h + (t-\alpha)^2 h' = (t-\alpha)(2h + (t-\alpha)h')$. So $f(\alpha) = f'(\alpha) = 0$. So f and f' have common roots. However, we want a common irreducible factor in $K[t]$, not $L[t]$. So we let P_α be the minimal polynomial of α over K. Then $P_\alpha \mid f$ and $P_\alpha \mid f'$. So done.

Conversely, suppose e is a common irreducible factor of f and f' in $K[t]$, with $\deg e > 0$. Pick $\alpha \in \mathrm{Root}_e(L)$. Then $\alpha \in \mathrm{Root}_f(L) \cap \mathrm{Root}_{f'}(L)$.

Since α is a root of f, we can write $f = (t-\alpha)q \in L[t]$ for some q. Then

$$f' = (t-\alpha)q' + q.$$

Since $(t-\alpha) \mid f'$, we must have $(t-\alpha) \mid q$. So $(t-\alpha)^2 \mid f$. □

Recall that the characteristic of a field $\operatorname{char} K$ is the minimum p such that $p \cdot 1_K = 0$. If no such p exists, we say $\operatorname{char} K = 0$. For example, $\mathbb{Q}$ has characteristic 0 while $\mathbb{Z}_p$ has characteristic p.

Corollary. Let K be a field, $f \in K[t]$ non-zero irreducible. Then

(i) If $\operatorname{char} K = 0$, then f is separable.

(ii) If $\operatorname{char} K = p > 0$, then f is not separable iff $\deg f > 0$ and $f \in K[t^p]$. For example, $t^{2p} + 3t^p + 1$ is not separable.

Proof. By definition, for irreducible f, f is not separable iff f has a repeated root. So by our previous lemma, f is not separable if and only if f and f' have a common irreducible factor of positive degree in $K[t]$. However, since f is irreducible, its only factors are 1 and itself. So this can happen if and only if $f' = 0$.

To make it more explicit, we can write

$$f = a_n t^n + \cdots + a_1 t + a_0.$$

Then we can write

$$f' = n a_n t^{n-1} + \cdots + a_1.$$

Now $f' = 0$ if and only if all coefficients $i a_i = 0$ for all i.

(i) Suppose $\operatorname{char} K = 0$, then if $\deg f = 0$, then f is trivially separable. If $\deg f > 0$, then f is not separable iff $f' = 0$ iff $i a_i = 0$ for all i iff $a_i = 0$ for $i \geq 1$. But we cannot have a polynomial of positive degree with all its coefficients zero (apart from the constant term). So f must be separable.

(ii) If $\deg f = 0$, then f is trivially separable. So assume $\deg f > 0$.

Then f is not separable $\Leftrightarrow f' = 0 \Leftrightarrow i a_i = 0$ for $i \geq 0 \Leftrightarrow a_i = 0$ for all $i \geq 1$ not multiples of $p \Leftrightarrow f \in K[t^p]$. □

Using this, it should be easy to find lots of examples of separable polynomials.

Definition (Separable elements and extensions)**.** Let $K \subseteq L$ be an algebraic field extension. We say $\alpha \in L$ is *separable* over K if P_α is separable, where P_α is the minimal polynomial of α over K.

We say L is *separable* over K (or $L \subseteq L$ is *separable*) if all $\alpha \in L$ are separable.

Example.

- The extensions $Q \subseteq \mathbb{Q}(\sqrt{2})$ and $\mathbb{R} \subseteq \mathbb{C}$ are separable because $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = 0$. So we can apply our previous corollary.
- Let $L = \mathbb{F}_p(s)$ be the field of rational functions in s over $\mathbb{F}_p$ (which is the fraction field of $\mathbb{F}_p[s]$), and $K = \mathbb{F}_p(s^p)$. We have $K \subseteq L$, and $L = K(s)$. Since $s^p \in K$, s is a root of $t^p - s^p \in K[t]$. So s is algebraic over K and hence L is algebraic over K. In fact $P_s = t^p - s^p$ is the minimal polynomial of s over K.

  Now $t^p - s^p = (t-s)^p$ since the field has characteristic p. So $\operatorname{Root}_{t^p - s^p}(L) = \{s\}$. So P_s is not separable.

As mentioned in the beginning, separable extensions are nice, or at least non-weird. One particular nice result about separable extensions is that all finite separable extensions are simple, i.e. if $K \subseteq L$ is finite separable, then $L = K(\alpha)$ for some $\alpha \in L$. This is what we will be working towards for the remaining of the section.

Example. Consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. This is a separable finite extension. So we should be able to generate $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ by just one element, not just two. In fact, we can use $\alpha = \sqrt{2} + \sqrt{3}$, since we have

$$\alpha^3 = 11\sqrt{2} + 9\sqrt{3} = 2\sqrt{2} + 9\alpha.$$

So since $\alpha^3 \in \mathbb{Q}(\alpha)$, we know that $\sqrt{2} \in \mathbb{Q}(\alpha)$. So we also have $\sqrt{3} \in \mathbb{Q}(\alpha)$.

In general, it is not easy to find an α that works, but we our later result will show that such an α exists.

Before that, we will prove some results about the K-homomorphisms.

Lemma. Let $L/F/K$ be finite extensions, and E/K be a field extension. Then for all $\alpha \in L$, we have

$$|\operatorname{Hom}_K(F(\alpha), E)| \leq [F(\alpha) : F] |\operatorname{Hom}_K(F, E)|.$$

Note that if P_α is the minimal polynomial of α over F, then $[F(\alpha) : F] = \deg P_\alpha$. So we can interpret this intuitively as follows: for each $\psi \in \operatorname{Hom}_K(F, E)$, we can obtain a K-homomorphism in $\operatorname{Hom}_K(F(\alpha), E)$ by sending things in F according to ψ, and then send α to any root of P_α. Then there are at most $[F(\alpha) : F]$ K-homomorphisms generated this way. Moreover, each K-homomorphism in $\operatorname{Hom}_K(F(\alpha), E)$ can be created this way. So we get this result.

Proof. We show that for each $\psi \in \operatorname{Hom}_K(F, E)$, there are at most $[F(\alpha) : F]$ K-isomorphisms in $\operatorname{Hom}_K(F(\alpha), E)$ that restrict to ψ in F. Since each K-isomorphism in $\operatorname{Hom}_K(F(\alpha), E)$ has to restrict to something, it follows that there are at most $[F(\alpha) : F] |\operatorname{Hom}_K(F, E)|$ K-homomorphisms from $F(\alpha)$ to E.

Now let P_α be the minimal polynomial for α in F, and let $\psi \in \mathrm{Hom}_K(F, E)$. To extend ψ to a morphism $F(\alpha) \to E$, we need to decide where to send α. So there should be some sort of correspondence

$$\mathrm{Root}_{P_\alpha}(E) \longleftrightarrow \{\phi \in \mathrm{Hom}_K(F(\alpha), E) : \phi|_F = \psi\}.$$

Except that the previous sentence makes no sense, since $P_\alpha \in F[t]$ but we are not told that F is a subfield of E. So we use our ψ to "move" our things to E.

We let $M = \psi(F) \subseteq E$, and $q \in M[t]$ be the image of P_α under the homomorphism $F[t] \to M[t]$ induced by ψ. As we have previously shown, there is a one-to-one correspondence

$$\mathrm{Root}_q(E) \longleftrightarrow \mathrm{Hom}_M(M[t]/\langle q\rangle, E).$$

What we really want to show is the correspondence between $\mathrm{Root}_q(E)$ and the K-homomorphisms $F[t]/\langle P_\alpha\rangle \to E$ that restrict to ψ on F. Let's ignore the quotient for the moment and think: what does it mean for $\phi \in \mathrm{Hom}_K(F[t], E)$ to restrict to ψ on F? We know that any $\phi \in \mathrm{Hom}_L(F[t], E)$ is uniquely determined by the values it takes on F and t. Hence if $\phi|_F = \psi$, then our ϕ must send F to $\psi(F) = M$, and can send t to anything in E. This corresponds exactly to the M-homomorphisms $M[t] \to E$ that does nothing to M and sends t to that "anything" in E.

The situation does not change when we put back the quotient. Changing from $M[t] \to E$ to $M[t]/\langle q\rangle \to E$ just requires that the image of t must be a root of q. On the other hand, using $F[t]/\langle P_\alpha\rangle$ instead of $F[t]$ requires that $\phi(P_\alpha(t)) = 0$. But we know that $\phi(P_\alpha) = \psi(P_\alpha) = q$. So this just requires $q(t) = 0$ as well. So we get the one-to-one correspondence

$$\mathrm{Hom}_M(M[t]/\langle q\rangle, E) \longleftrightarrow \{\phi \in \mathrm{Hom}_K(F[t]/\langle P_\alpha\rangle, E) : \phi|_F = \psi\}.$$

Since $F[t]/\langle P_\alpha\rangle = F(\alpha)$, there is a one-to-one correspondence

$$\mathrm{Root}_q(E) \longleftrightarrow \{\phi \in \mathrm{Hom}_K(F(\alpha), E) : \phi|_F = \psi\}.$$

So done. □

Theorem. Let L/K and E/K be field extensions. Then

(i) $|\mathrm{Hom}_K(L, E)| \leq [L : K]$. In particular, $|\mathrm{Aut}_K(L)| \leq [L : K]$.

(ii) If equality holds in (i), then for any intermediate field $K \subseteq F \subseteq L$:

  (a) We also have $|\mathrm{Hom}_K(F, E)| = [F : K]$.

  (b) The map $\mathrm{Hom}_K(L, E) \to \mathrm{Hom}_K(F, E)$ by restriction is surjective.

Proof.

(i) We have previously shown we can find a sequence of field extensions

$$K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = L$$

such that for each i, there is some α_i such that $F_i = F_{i-1}(\alpha_i)$. Then by our previous lemma, we have

$$\begin{aligned}
|\operatorname{Hom}_K(L, E)| &\leq [F_n : F_{n-1}]|\operatorname{Hom}_K(F_{n-1}, E)| \\
&\leq [F_n : F_{n-1}][F_{n-1} : F_{n-2}]|\operatorname{Hom}_K(F_{n-2}, E)| \\
&\vdots \\
&\leq [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \cdots [F_1 : F_0]|\operatorname{Hom}_K(F_0, E)| \\
&= [F_n : F_0] \\
&= [L : K]
\end{aligned}$$

(ii) (a) If equality holds in (i), then every inequality in the proof above has to an equality. Instead of directly decomposing $K \subseteq L$ as a chain above, we can first decompose $K \subseteq F$, then $F \subseteq L$, then join them together. Then we can assume that $F = F_i$ for some i. Then we get

$$|\operatorname{Hom}_K(L, E)| = [L : F]|\operatorname{Hom}_K(F, E)| = [L : K].$$

Then the tower law says

$$|\operatorname{Hom}_K(F, E)| = [F : K].$$

(b) By the proof of the lemma, for each $\psi \in \operatorname{Hom}_K(F, E)$, we know that

$$\{\phi : \operatorname{Hom}_K(L, E) : \phi|_F = \psi\} \leq [L : F]. \qquad (*)$$

As we know that

$$|\operatorname{Hom}_K(F, E)| = [F : K], \quad |\operatorname{Hom}_K(L, E)| = [L : K]$$

we must have had equality in $(*)$, or else we won't have enough elements. So in particular $\{\phi : \operatorname{Hom}_K(L, E) : \phi|_F = \psi\} \geq 1$. So the map is surjective. □

With this result, we can prove prove the following result characterizing separable *extensions*.

Theorem. Let L/K be a finite field extension. Then the following are equivalent:

(i) There is some extension E of K such that $|\operatorname{Hom}_K(L, E)| = [L : K]$.

(ii) L/K is separable.

(iii) $L = K(\alpha_1, \cdots, \alpha_n)$ such that P_{α_i}, the minimal polynomial of α_i over K, is separable for all i.

(iv) $L = K(\alpha_1, \cdots, \alpha_n)$ such that R_{α_i}, the minimal polynomial of α_i over $K(\alpha_1, \cdots, \alpha_{i-1})$ is separable for all i for all i.

Proof.

– (i) ⇒ (ii): For all $\alpha \in L$, if P_α is the minimal polynomial of α over K, then since $K(\alpha)$ is a subfield of L, by our previous theorem, we have

$$|\operatorname{Hom}_K(K(\alpha), E)| = [K(\alpha) : K].$$

We also know that $|\operatorname{Root}_{P_\alpha}(E)| = |\operatorname{Hom}_K(K(\alpha), E)|$, and that $[K(\alpha) : K] = \deg P_\alpha$. So we know that P_α has no repeated roots in any splitting field. So P_α is a separable. So L/K is a separable extension.

– (ii) ⇒ (iii): Obvious from definition

– (iii) ⇒ (iv): Since R_{α_i} is a minimal polynomial in $K(\alpha_1, \cdots, \alpha_{i-1})$, we know that $R_{\alpha_i} \mid P_{\alpha_i}$. So R_{α_i} is separable as P_{α_i} is separable.

– (iv) ⇒ (i): Let E be the splitting field of $P_{\alpha_1}, \cdots, P_{\alpha_n}$. We do induction on n to show that this satisfies the properties we want. If $n = 1$, then $L = K(\alpha_1)$. Then we have

$$|\operatorname{Hom}_K(L, E)| = |\operatorname{Root}_{P_{\alpha_i}}(E)| = \deg P_{\alpha_1} = [K(\alpha_1) : K] = [L : K].$$

We now induct on n. So we can assume that (iv) ⇒ (i) holds for smaller number of generators. For convenience, we write $K_i = K(\alpha_1, \cdots, \alpha_i)$. Then we have

$$|\operatorname{Hom}_K(K_{n-1}, E)| = [K_{n-1} : K].$$

We also know that

$$|\operatorname{Hom}_K(K_n, E)| \leq [K_n : K_{n-1}]|\operatorname{Hom}_K(K_{n-1}, E)|.$$

What we actually want is equality. We now re-do (parts of) the proof of this result, and see that separability guarantees that equality holds. If we pick $\psi \in \operatorname{Hom}_K(K_{n-1}, E)$, then there is a one-to-one correspondence between $\{\phi \in \operatorname{Hom}_K(K_n, E) : \phi|_{K_{n-1}} = \psi\}$ and $\operatorname{Root}_q(E)$, where $q \in M[t]$ is defined as the image of R_{α_n} under $K_{n-1}[t] \to M[t]$, and M is the image of ψ.

Since $P_{\alpha_n} \in K[t]$ and $R_{\alpha_n} \mid P_{\alpha_n}$, then $q \mid P_{\alpha_n}$. So q splits over E. By separability assumption , we get that

$$|\operatorname{Root}_q(E)| = \deg q = \deg R_{\alpha_n} = [K_n : K_{n-1}].$$

Hence we know that

$$\begin{aligned} |\operatorname{Hom}_K(L, E)| &= [K_n : K_{n-1}]|\operatorname{Hom}_K(K_{n-1}, E)| \\ &= [K_n : K_{n-1}][K_{n-1} : K] \\ &= [K_n : K]. \end{aligned}$$

So done. □

Before we finally get to the primitive element theorem, we prove the following lemma. This will enable us to prove the trivial case of the primitive element theorem, and will also be very useful later on.

Lemma. Let L be a field, $L^* \setminus \{0\}$ be the multiplicative group of L. If G is a finite subgroup of L^*, then G is cyclic.

Proof. Since L^* is abelian, G is also abelian. Then by the structure theorem on finite abelian groups,

$$G \cong \frac{\mathbb{Z}}{\langle n_1 \rangle} \times \cdots \times \frac{\mathbb{Z}}{\langle n_r \rangle},$$

for some $n_i \in \mathbb{N}$. Let m be the least common multiple of $n_1, \cdots, n_r$, and let $f = t^m - 1$.

If $\alpha \in G$, then $\alpha^m = 1$. So $f(\alpha) = 0$ for all $\alpha \in G$. Therefore

$$|G| = n_1 \cdots n_r \leq |\operatorname{Root}_f(L)| \leq \deg f = m.$$

Since m is the least common multiple of $n_1, \cdots, n_r$, we must have $m = n_1 \cdots n_r$ and thus $(n_i, n_j) = 1$ for all $i \neq j$. Then by the Chinese remainder theorem, we have

$$G \cong \frac{Z}{\langle n_1 \rangle} \times \cdots \times \frac{\mathbb{Z}}{\langle n_r \rangle} = \frac{\mathbb{Z}}{\langle n_1 \cdots n_r \rangle}.$$

So G is cyclic. □

We now come to the main theorem of the lecture:

Theorem (Primitive element theorem)**.** Assume L/K is a finite and separable extension. Then L/K is simple, i.e. there is some $\alpha \in L$ such that $L = K(\alpha)$.

Proof. At some point in our proof, we will require that L is infinite. So we first do the finite case first. If K is finite, then L is also finite, which in turns implies L^* is finite too. So by the lemma, L^* is a cyclic group (since it is a finite subgroup of itself). So there is some $\alpha \in L^*$ such that every element in L^* is a power of α. So $L = K(\alpha)$.

So focus on the case where K is infinite. Also, assume $K \neq L$. Then since L/K is a finite extension, there is some intermediate field $K \subseteq F \subsetneq L$ such that $L = F(\beta)$ for some β. Now L/K is separable. So F/K is also separable, and $[F : K] < [L : K]$. Then by induction on degree of extension, we can assume F/K is simple. In other words, there is some $\lambda \in F$ such that $F = K(\lambda)$. Now $L = K(\lambda, \beta)$. In the rest of the proof, we will try to replace the two generators λ, β with just a single generator.

Unsurprisingly, the generator of L will be chosen to be a linear combination of β and λ. We set

$$\alpha = \beta + a\lambda$$

for some $a \in K$ to be chosen later. We will show that $K(\alpha) = L$. Actually, almost any choice of a will do, but at the end of the proof, we will see which ones are the bad ones.

Let P_β and P_λ be the minimal polynomial of β and λ over K respectively. Consider the polynomial $f = P_\beta(\alpha - at) \in K(\alpha)[t]$. Then we have

$$f(\lambda) = P_\beta(\alpha - a\lambda) = P_\beta(\beta) = 0.$$

On the other hand, $P_\lambda(\lambda) = 0$. So λ is a common root of P_λ and f.

We now want to pick an a such that λ is the *only* common root of f and P_λ (in E). If so, then the gcd of f and P_α in $K(\alpha)$ must only have λ as a root. But since P_λ is separable, it has no double roots. So the gcd must be $t - \lambda$. In particular, we must have $\lambda \in K(\alpha)$. Since $\alpha = \beta + a\lambda$, it follows that $\beta \in K(\alpha)$ as well, and so $K(\alpha) = L$.

Thus, it remains to choose an a such that there are no other common roots. We work in a splitting field of $P_\beta P_\lambda$, and write

$$P_\beta = (t-\beta_1)\cdots(t-\beta_m)$$
$$P_\lambda = (t-\lambda_1)\cdots(t-\lambda_n).$$

We wlog $\beta_1 = \beta$ and $\lambda_1 = \lambda$.

Now suppose θ is a common root of f and P_λ. Then

$$\begin{cases} f(\theta) = 0 \\ P_\lambda(\theta) = 0 \end{cases} \Rightarrow \begin{cases} P_\beta(\alpha - a\theta) = 0 \\ P_\lambda(\theta) = 0 \end{cases} \Rightarrow \begin{cases} \alpha - a\theta = \beta_i \\ \theta = \lambda_j \end{cases}$$

for some i, j. Then we know that

$$\alpha = \beta_i + a\lambda_j.$$

However, by definition, we also know that

$$\alpha = \beta + a\lambda$$

Now we see how we need to choose a. We need to choose a such that the elements

$$\beta + a\lambda \neq \beta_i + a\lambda_j$$

for all i, j. But if they were equal, then we have

$$a = \frac{\lambda - \lambda_j}{\beta_i - \beta},$$

and there are only finitely many elements of this form. So we just have to pick an *a not* in this list. □

Corollary. Any finite extension L/K of field of characteristic 0 is simple, i.e. $L = K(\alpha)$ for some $\alpha \in L$.

Proof. This follows from the fact that all extensions of fields of characteristic zero are separable. □

We have previously seen that $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is a simple extension, but that is of course true from this theorem. A more interesting example would be one in which this fails. We will need a field with non-zero characteristic.

Example. Let $L = \mathbb{F}_p(s, u)$, the fraction field of $\mathbb{F}_p[s, u]$. Let $K = \mathbb{F}_p(s^p, u^p)$. We have L/K. We want to show this is not simple.

If $\alpha \in L$, then $\alpha^p \in K$. So α is a root of $t^p - \alpha^p \in K[t]$. Thus the minimal polynomial P_α has degree at most p. So $[K(\alpha) : K] = \deg P_\alpha \leq p$. On the other hand, we have $[L : K] = p^2$, since $\{s^i u^j : 0 \leq i, j < p\}$ is a basis. So for any α, we have $K(\alpha) \neq L$. So L/K is not a simple extension. This then implies L/K is not separable.

At this point, one might suspect that all fields with positive characteristic are not separable. This is not true by considering a rather silly example.

Example. Consider $K = \mathbb{F}_2$ and $L = \mathbb{F}_2[s]/\langle s^2 + s + 1\rangle$. We can check manually that $s^2 + s + 1$ has no roots and hence irreducible. So L is a field. So $L/\mathbb{F}_2$ is a finite extension. Note that L only has 4 elements.

Now if $\alpha \in L \setminus \mathbb{F}_2$, and P_α is the minimal polynomial of α over $\mathbb{F}_2$, then $P_\alpha \mid t^2 + t + 1$. So P_α is separable as a polynomial. So $L/\mathbb{F}_2$ is separable.

In fact, we have

Proposition. Let L/K be an extension of finite fields. Then the extension is separable.

Proof. Let the characteristic of the fields be p. Suppose the extension were not separable. Then there is some non-separable element $\alpha \in L$. Then its minimal polynomial must be of the form $P_\alpha = \sum a_i t^{pi}$.

Now note that the map $K \to K$ given by $x \mapsto x^p$ is injective, hence surjective. So we can write $a_i = b_i^p$ for all i. Then we have

$$P_\alpha = \sum a_i t^{pi} = \left(\sum b_i t^i\right)^p,$$

and so P_α is not irreducible, which is a contradiction. □

2.7 Normal extensions

We are almost there. We will now move on to study normal extensions. Normal extensions are *very* closely related to Galois extensions. In fact, we will show that if an extension is normal and separable, then it is Galois. The advantage of introducing the idea of normality is that normality is a much more concrete definition to work with. It is much easier to check if an extension is normal than to check if $|\operatorname{Aut}_K(L)| = [K : L]$. In particular, we will shortly prove that the splitting field of any polynomial is normal.

This is an important result, since we are going to use the splitting field to study the roots of a polynomial, and since we mostly care about polynomials over $\mathbb{Q}$, this means all these splitting fields are automatically Galois extensions of $\mathbb{Q}$.

It is not immediately obvious why these extensions are called "normal" (just like most other names in Galois theory). We will later see that normal extensions are extensions that correspond to normal subgroups, in some precise sense given by the fundamental theorem of Galois theory.

Definition (Normal extension)**.** Let $K \subseteq L$ be an algebraic extension. We say L/K is *normal* if for all $\alpha \in L$, the minimal polynomial of α over K splits over L.

In other words, given any minimal polynomial, L should have all its roots.

Example. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal since the minimal polynomial $t^3 - 2$ does not split over $\mathbb{Q}(\sqrt[3]{2})$.

In some sense, extensions that are not "normal" are missing something. This is somewhat similar to how Galois extensions work. Before we go deeper into this, we need a lemma.

Lemma. Let $L/F/K$ be finite extensions, and $\bar{K}$ is the algebraic closure of K. Then any $\psi \in \operatorname{Hom}_K(F, \bar{K})$ extends to some $\phi \in \operatorname{Hom}_K(L, \bar{K})$.

Proof. Let $\psi \in \mathrm{Hom}_K(F, \bar{K})$. If $F = L$, then the statement is trivial. So assume $L \neq F$.

Pick $\alpha \in L \setminus F$. Let $q_\alpha \in F[t]$ be the minimal polynomial of α over F. Consider $\psi(q_\alpha) \in \bar{K}[t]$. Let β be any root of q_α, which exists since $\bar{K}$ is algebraically closed. Then as before, we can extend ψ to $F(\alpha)$ by sending α to β. More explicitly, we send

$$\sum_{i=0}^{N} a_i \alpha^i \mapsto \sum \psi(a_i)\beta^i,$$

which is well-defined since any polynomial relation satisfied by α in F is also satisfied by β.

Repeat this process finitely many times to get some element in $\mathrm{Hom}_K(L, \bar{K})$. □

We will use this lemma to characterize normal extensions.

Theorem. Let L/K be a finite extension. Then L/K is a normal extension if and only if L is the splitting field of some $f \in K[t]$.

Proof. Suppose L/K is normal. Since L is finite, let $L = K(\alpha_1, \cdots, \alpha_n)$ for some $\alpha_i \in L$. Let P_{α_i} be the minimal polynomial of α_i over K. Take $f = P_{\alpha_1} \cdots P_{\alpha_n}$. Since L/K is normal, each P_{α_i} splits over L. So f splits over L, and L is a splitting field of f.

For the other direction, suppose that L is the splitting field of some $f \in K[t]$. First we wlog assume $L \subseteq \bar{K}$. This is possible since the natural injection $K \hookrightarrow \bar{K}$ extends to some $\phi : L \to \bar{K}$ by our previous lemma, and we can replace L with $\phi(L)$.

Now suppose $\beta \in L$, and let P_β be its minimal polynomial. Let β' be another root. We want to show it lives in L.

Now consider $K(\beta)$. By the proof of the lemma, we can produce an embedding $\iota : K(\beta) \to \bar{K}$ that sends β to β'. By the lemma again, this extends to an embedding of L into $\bar{K}$. But any such embedding must send a root of f to a root of f. So it must send L to L. In particular, $\iota(\beta) = \beta' \in L$. So P_β splits over L. □

This allows us to identify normal extensions easily. The following theorem then allows us to identify *Galois* extensions using this convenient tool.

Theorem. Let L/K be a finite extension. Then the following are equivalent:

(i) L/K is a Galois extension.

(ii) L/K is separable and normal.

(iii) $L = K(\alpha_1, \cdots, \alpha_n)$ and P_{α_i}, the minimal polynomial of α_i over K, is separable and splits over L for all i.

Proof.

– (i) ⇒ (ii): Suppose L/K is a Galois extension. Then by definition, this means

$$|\,\mathrm{Hom}_K(L, L)| = |\,\mathrm{Aut}_K(L)| = [L : K].$$

To show that L/K is separable, recall that we proved that an extension is separable if and only if there is some E such that $|\operatorname{Hom}_K(L, E)| = [L : K]$. In this case, just pick $E = L$. Then we know that the extension is separable.

To check normality, let $\alpha \in L$, and let P_α be its minimal polynomial over K. We know that

$$|\operatorname{Root}_{P_\alpha}(L)| = |\operatorname{Hom}_K(K[t]/\langle P_\alpha\rangle, L)| = |\operatorname{Hom}_K(K(\alpha), L)|.$$

But since $|\operatorname{Hom}_K(L, L)| = [L : K]$ and $K(\alpha)$ is a subfield of L, this implies

$$|\operatorname{Hom}_K(K(\alpha), L)| = [K(\alpha) : K] = \deg P_\alpha.$$

Hence we know that

$$|\operatorname{Root}_{P_\alpha}(L)| = \deg P_\alpha.$$

So P_α splits over L.

– (ii) $\Rightarrow$ (iii): Just pick $\alpha_1, \cdots, \alpha_n$ such that $L = K(\alpha_1, \cdots, \alpha_n)$. Then these polynomials are separable since the extension is separable, and they split since L/K is normal. In fact, by the primitive element theorem, we can pick these such that $n = 1$.

– (iii) $\Rightarrow$ (i): Since $L = K(\alpha_1, \cdots, \alpha_n)$ and the minimal polynomials P_{α_i} over K are separable, by a previous theorem, there are some extension E of K such that

$$|\operatorname{Hom}_K(L, E)| = [L : K].$$

To simplify notation, we first replace L with its image inside E under some K-homomorphism $L \to E$, which exists since $|\operatorname{Hom}_K(L, E)| = [L : K] > 0$. So we can assume $L \subseteq E$.

We now claim that the inclusion

$$\operatorname{Hom}_K(L, L) \to \operatorname{Hom}_K(L, E)$$

is a surjection, hence a bijection. Indeed, if $\phi : L \to E$, then ϕ takes α_i to $\phi(\alpha_i)$, which is a root of P_{α_i}. Since P_{α_i} splits over L, we know $\phi(\alpha_i) \in L$ for all i. Since L is generated by these α_i, it follows that $\phi(L) \subseteq L$.

Thus, we have

$$[L : K] = |\operatorname{Hom}_K(L, E)| = |\operatorname{Hom}_K(L, L)|,$$

and the extension is Galois. □

From this, it follows that if L/K is Galois, and we have an intermediate field $K \subseteq F \subseteq L$, then L/F is also Galois.

Corollary. Let K be a field and $f \in K[t]$ be a separable polynomial. Then the splitting field of f is Galois.

This is one of the most crucial examples.

2.8 The fundamental theorem of Galois theory

Finally, we can get to the fundamental theorem of Galois theory. Roughly, given a Galois extension $K \subseteq L$, the fundamental theorem tell us there is a one-to-one correspondence between intermediate field extensions $K \subseteq F \subseteq L$ and subgroups of the automorphism group $\mathrm{Gal}(L/K)$.

Given an intermediate field F, we can obtain a subgroup of $\mathrm{Gal}(L/K)$ by looking at the automorphisms that fix F. To go the other way round, given a subgroup $H \leq \mathrm{Gal}(L/K)$, we can obtain a corresponding field by looking at the field of elements that are fixed by everything in H. This is known as the *fixed field*, and can in general be defined even for non-Galois extensions.

Definition (Fixed field)**.** Let L/K be a field extension, $H \leq \mathrm{Aut}_K(L)$ a subgroup. We define the *fixed field* of H as

$$L^H = \{\alpha \in L : \phi(\alpha) = \alpha \text{ for all } \phi \in H\}.$$

It is easy to see that L^H is an intermediate field $K \subseteq L^H \subseteq L$.

Before we get to the fundamental theorem, we first prove *Artin's lemma*. This in fact proves part of the results in the fundamental theorem, but is also useful on its own right.

Lemma (Artin's lemma)**.** Let L/K be a field extension and $H \leq \mathrm{Aut}_K(L)$ a finite subgroup. Then L/L^H is a Galois extension with $\mathrm{Aut}_{L^H}(L) = H$.

Note that we are not assuming that L/K is Galois, or even finite!

Proof. Pick any $\alpha \in L$. We set

$$\{\alpha_1, \cdots, \alpha_n\} = \{\phi(\alpha) : \phi \in H\},$$

where α_i are distinct. Here we are allowing for the possibility that $\phi(\alpha) = \psi(\alpha)$ for some distinct $\phi, \psi \in H$.

By definition, we clearly have $n < |H|$. Let

$$f = \prod_1^n (t - \alpha_i) \in L[t].$$

We know that any $\phi \in H$ gives an homomorphism $L[t] \to L[t]$, and any such map fixes f because ϕ just permutes the α_i. Thus, the coefficients of f are in L^H, and thus $f \in L^H[t]$.

Since $\mathrm{id} \in H$, we know that $f(\alpha) = 0$. So α is algebraic over L^H. Moreover, if q_α is the minimal polynomial of α over L^H, then $q_\alpha \mid f$ in $L^H[t]$. Hence

$$[L^H(\alpha) : L^H] = \deg q_\alpha \leq \deg f \leq |H|.$$

Further, we know that f has distinct roots. So q_α is separable, and so α is separable. So it follows that L/L^H is a separable extension.

We next show that L/L^H is simple. This doesn't immediately follow from the primitive element theorem, because we don't know it is a finite extension yet, but we can still apply the theorem cleverly.

Pick $\alpha \in L$ such that $[L^H(\alpha) : L^H]$ is maximal. This is possible since $[L^H(\alpha) : L^H]$ is bounded by $|H|$. The claim is that $L = L^H(\alpha)$.

We pick an arbitrary $\beta \in L$, and will show that this is in $L^H(\alpha)$. By the above arguments, $L^H \subseteq L^H(\alpha, \beta)$ is a finite separable extension. So by the primitive element theorem, there is some $\lambda \in L$ such that $L^H(\alpha, \beta) = L^H(\lambda)$. Note that we must have

$$[L^H(\lambda) : L^H] \geq [L^H(\alpha) : L^H].$$

By maximality of $[L^H(\alpha) : L^H]$, we must have equality. So $L^H(\lambda) = L^H(\alpha)$. So $\beta \in L^H(\alpha)$. So $L = L^H(\alpha)$.

Finally, we show it is a Galois extension. Let $L = L^H(\alpha)$. Then

$$[L : L^H] = [L^H(\alpha) : L^H] \leq |H| \leq |\operatorname{Aut}_{L^H}(L)|$$

Recall that we have previously shown that for any extension L/L^H, we have $|\operatorname{Aut}_{L^H}(L)| \leq [L : L^H]$. Hence we must have equality above. So

$$[L : L^H] = |\operatorname{Aut}_{L^H}(L)|.$$

So the extension is Galois. Also, since we know that $H \subseteq \operatorname{Aut}_{L^H}(L)$, we must have $H = \operatorname{Aut}_{L^H}(L)$. □

Theorem. Let L/K be a finite field extension. Then L/K is Galois if and only if $L^H = K$, where $H = \operatorname{Aut}_K(L)$.

Proof. ($\Rightarrow$) Suppose L/K is a Galois extension. We want to show $L^H = K$. Using Artin's lemma (and the definition of H), we have

$$[L : K] = |\operatorname{Aut}_K(L)| = |H| = |\operatorname{Aut}_{L^H}(L)| = [L : L^H]$$

So $[L : K] = [L : L^H]$. So we must have $L^H = K$.

($\Leftarrow$) By the lemma, $K = L^H \subseteq L$ is Galois. □

This is an important theorem. Given a Galois extension L/K, this gives us a very useful test of when elements of $\alpha \in L$ are in fact in K. We will use this a lot.

Finally, we get to the fundamental theorem.

Theorem (Fundamental theorem of Galois theory)**.** Assume L/K is a (finite) Galois extension. Then

(i) There is a one-to-one correspondence

$$H \leq \operatorname{Aut}_K(L) \longleftrightarrow \text{intermediate fields } K \subseteq F \subseteq L.$$

This is given by the maps $H \mapsto L^H$ and $F \mapsto \operatorname{Aut}_F(L)$ respectively. Moreover, $|\operatorname{Aut}_K(L) : H| = [L^H : K]$.

(ii) $H \leq \operatorname{Aut}_K(L)$ is normal (as a subgroup) if and only if L^H/K is a normal extension if and only if L^H/K is a Galois extension.

(iii) If $H \lhd \operatorname{Aut}_K(L)$, then the map $\operatorname{Aut}_K(L) \to \operatorname{Aut}_K(L^H)$ by the restriction map is well-defined and surjective with kernel isomorphic to H, i.e.

$$\frac{\operatorname{Aut}_K(L)}{H} = \operatorname{Aut}_K(L^H).$$

Proof. Note that since L/K is a Galois extension, we know

$$|\operatorname{Aut}_K(L)| = |\operatorname{Hom}_K(L, L)| = [L : K],$$

By a previous theorem, for any intermediate field $K \subseteq F \subseteq L$, we know $|\operatorname{Hom}_K(F, L)| = [F : K]$ and the restriction map $\operatorname{Hom}_K(L, L) \to \operatorname{Hom}_K(F, L)$ is surjective.

(i) The maps are already well-defined, so we just have to show that the maps are inverses to each other. By Artin's lemma, we know that $H = \operatorname{Aut}_{L^H}(L)$, and since L/F is a Galois extension, the previous theorem tells that $L^{\operatorname{Aut}_F(L)} = F$. So they are indeed inverses. The formula relating the index and the degree follows from Artin's lemma.

(ii) Note that for every $\phi \in \operatorname{Aut}_K(L)$, we have that $L^{\phi H \phi^{-1}} = \phi L^H$, since $\alpha \in L^{\phi H \phi^{-1}}$ iff $\phi(\psi(\phi^{-1}(\alpha))) = \alpha$ for all $\psi \in H$ iff $\psi(\phi^{-1}(\alpha)) = \phi^{-1}(\alpha)$ for all $\psi \in H$ iff $\alpha \in \phi L^H$. Hence H is a normal subgroup if and only if

$$\phi(L^H) = L^H \text{ for all } \phi \in \operatorname{Aut}_K(L). \qquad (*)$$

Assume $(*)$. We want to first show that $\operatorname{Hom}_K(L^H, L^H) = \operatorname{Hom}_K(L^H, L)$. Let $\psi \in \operatorname{Hom}_K(L^H, L)$. Then by the surjectivity of the restriction map $\operatorname{Hom}_K(L, L) \to \operatorname{Hom}_K(L^H, L)$, ψ must be the restriction of some $\tilde{\psi} \in \operatorname{Hom}_K(L, L)$. So $\tilde{\psi}$ fixes L^H by $(*)$. So ψ sends L^H to L^H. So $\psi \in \operatorname{Hom}_K(L^H, L^H)$. So we have

$$|\operatorname{Aut}_K(L^H)| = |\operatorname{Hom}_K(L^H, L^H)| = |\operatorname{Hom}_K(L^H, L)| = [L^H : K].$$

So L^H/K is Galois, and hence normal.

Now suppose L^H/K is a normal extension. We want to show this implies $(*)$. Pick any $\alpha \in L^H$ and $\phi \in \operatorname{Aut}_K(L)$. Let P_α be the minimal polynomial of α over K. So $\phi(\alpha)$ is a root of P_α (since ϕ fixes $P_\alpha \in K$, and hence maps roots to roots). Since L^H/K is normal, P_α splits over L^H. This implies that $\phi(\alpha) \in L^H$. So $\phi(L^H) = L^H$.

Hence, H is a normal subgroup if and only if $\phi(L^H) = L^H$ if and only if L^H/K is a Galois extension.

(iii) Suppose H is normal. We know that $\operatorname{Aut}_K(L) = \operatorname{Hom}_K(L, L)$ restricts to $\operatorname{Hom}_K(L^H, L)$ surjectively. To show that we in fact have restriction to $\operatorname{Aut}_K(L^H)$, by the proof above, we know that $\phi(L^H) = L^H$ for all $\phi \in \operatorname{Aut}_K(L^H)$. So this does restrict to an automorphism of L^H. In other words, the map $\operatorname{Aut}_K(L) \to \operatorname{Aut}_K(L^H)$ is well-defined. It is easy to see this is a group homomorphism.

Finally, we have to calculate the kernel of this homomorphism. Let E be the kernel. Then by definition, $E \supseteq H$. So it suffices to show that $|E| = |H|$. By surjectivity of the map and the first isomorphism theorem of groups, we have

$$\frac{|\operatorname{Aut}_K(L)|}{|E|} = |\operatorname{Aut}_K(L^H)| = [L^H : K] = \frac{[L : K]}{[L : L^H]} = \frac{|\operatorname{Aut}_K(L)|}{|H|},$$

noting that L^H/K and L/K are both Galois extensions, and $|H| = [L^H : K]$ by Artin's lemma. So $|E| = |H|$. So we must have $E = H$. □

Example. Let p be an odd prime, and ζ_p be a primitive pth root of unity. Given a (square-free) integer n, when is $\sqrt{n}$ in $\mathbb{Q}(\zeta_p)$? We know that $\sqrt{n} \in \mathbb{Q}(\zeta_p)$ if and only if $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_p)$. Moreover, $[\mathbb{Q}(\sqrt{n}) : \mathbb{Q}] = 2$, i.e. $\mathbb{Q}(\sqrt{n})$ is a quadratic extension.

We will later show that $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}$. Then by the fundamental theorem of Galois theory, quadratic extensions contained in $\mathbb{Q}(\zeta_p)$ correspond to index 2-subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. By general group theory, there is exactly one such subgroup. So there is exactly one square-free n such that $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_p)$ (since all quadratic extensions are of the form $\mathbb{Q}(\sqrt{n})$), given by the fixed field of the index 2 subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$.

Now we shall try to find some square root lying in $\mathbb{Q}(\zeta_p)$. We will not fully justify the derivation, since we can just square the resulting number to see that it is correct. We know the general element of $\mathbb{Q}(\zeta_p)$ looks like

$$\sum_{k=0}^{p-1} c_k \zeta_p^k.$$

We know $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$ acts by sending $\zeta_p \mapsto \zeta_p^n$ for each $n \in (\mathbb{Z}/p\mathbb{Z})^*$, and the index 2 subgroup consists of the quadratic residues. Thus, if an element is fixed under the action of the quadratic residues, the quadratic residue powers all have the same coefficient, and similarly for the non-residue powers.

If we wanted this to be a square root, then the action of the remaining elements of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ should negate this object. Since these elements swap the residues and the non-residues, we would want to have something like $c_k = 1$ if k is a quadratic residue, and -1 if it is a non-residue, which is just the Legendre symbol! So we are led to try to square

$$\tau = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta_p^k.$$

It is an exercise in the Number Theory example sheet to show that the square of this is in fact

$$\tau^2 = \left(\frac{-1}{p}\right) p.$$

So we have $\sqrt{p} \in \mathbb{Q}(\zeta_p)$ if $p \equiv 1 \pmod 4$, and $\sqrt{-p} \in \mathbb{Q}(\zeta_p)$ if $p \equiv 3 \pmod 4$.

2.9 Finite fields

We'll have a slight digression and look at finite fields. We adopt the notation where p is always a prime number, and $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$. It turns out finite fields are rather simple, as described in the lemma below:

Lemma. Let X be a finite field with $q = |K|$ element. Then

(i) $q = p^d$ for some $d \in \mathbb{N}$, where $p = \mathrm{char}\, K > 0$.

(ii) Let $f = t^q - t$. Then $f(\alpha) = 0$ for all $\alpha \in K$. Moreover, K is the splitting field of f over $\mathbb{F}_p$.

This means that a finite field is completely determined by the number of elements.

Proof.

(i) Consider the set $\{m \cdot 1_K\}_{m\in\mathbb{Z}}$, where 1_K is the unit in K and $m\cdot$ represents repeated addition. We can identify this with $\mathbb{F}_p$. So we have the extension $\mathbb{F}_p \subseteq K$. Let $d = [K : \mathbb{F}_p]$. Then $q = |K| = p^d$.

(ii) Note that $K^* = K \setminus \{0\}$ is a finite multiplicative group with order $q - 1$. Then by Lagrange's theorem, $\alpha^{q-1} = 1$ for all $\alpha \in K^*$. So $\alpha^q - \alpha = 0$ for all $\alpha \neq 0$. The $\alpha = 0$ case is trivial.

Now every element in K is a root of f. So we need to check that all roots of f are in K. Note that the derivative $f' = qt^{q-1} - 1 = -1$ (since q is a power of the characteristic). So $f'(\alpha) = -1 \neq 0$ for all $\alpha \in K$. So f and f' have no common roots. So f has no repeated roots. So K contains q distinct roots of f. So K is a splitting field. □

Lemma. Let $q = p^d$, $q' = p^{d'}$, where $d, d' \in \mathbb{N}$. Then

(i) There is a finite field K with exactly q elements, which is unique up to isomorphism. We write this as $\mathbb{F}_q$.

(ii) We can embed $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ iff $d \mid d'$.

Proof.

(i) Let $f = t^q - t$, and let K be a splitting field of f over $\mathbb{F}_p$. Let $L = \operatorname{Root}_f(K)$. The objective is to show that $L = K$. Then we will have $|K| = |L| = |\operatorname{Root}_f(K)| = \deg f = q$, because the proof of the previous lemma shows that f has no repeated roots.

To show that $L = K$, by definition, we have $L \subseteq K$. So we need to show every element in K is in L. We do so by showing that L itself is a field. Then since L contains all the roots of f and is a subfield of the splitting field K, we must have $K = L$.

It is straightforward to show that L is a field: if $\alpha, \beta \in L$, then

$$(\alpha + \beta)^q = \alpha^q + \beta^q = \alpha + \beta.$$

So $\alpha + \beta \in L$. Similarly, we have

$$(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta.$$

So $\alpha\beta \in L$. Also, we have

$$(\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}.$$

So $\alpha^{-1} \in L$. So L is in fact a field.

Since any field of size q is a splitting field of f, and splitting fields are unique to isomorphism, we know that K is unique.

(ii) Suppose $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$. Then let $n = [\mathbb{F}_{q'} : \mathbb{F}_q]$. So $q' = q^n$. So $d' = nd$. So $d \mid d'$.

On the other hand, suppose $d \mid d'$. Let $d' = dn$. We let $f = t^{q'} - t$. Then for any $\alpha \in \mathbb{F}_q$, we have

$$f(\alpha) = \alpha^{q'} - \alpha = \alpha^{q^n} - \alpha = (\cdots((\alpha^q)^q)^q \cdots)^q - \alpha = \alpha - \alpha = 0.$$

Since $\mathbb{F}_{q'}$ is the splitting field of f, all roots of f are in $\mathbb{F}_{q'}$. So we know that $\mathbb{F}_q \subseteq \mathbb{F}'_q$. □

Note that if $\bar{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$, then $\mathbb{F}_q \subseteq \bar{F}_p$ for every $q = p^d$. We then have

$$\bigcup_{k\in\mathbb{N}} \mathbb{F}_{p^k} = \bar{\mathbb{F}}_p,$$

because any $\alpha \in \bar{\mathbb{F}}_p$ is algebraic over $\mathbb{F}_p$, and so belongs to some $\mathbb{F}_q$.

Definition. Consider the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, where q is a power of p. The *Frobenius* $\mathrm{Fr}_q : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is defined by $\alpha \mapsto \alpha^q$.

This is a homomorphism precisely because the field is of characteristic zero. In fact, $\mathrm{Fr}_q \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$, since $\alpha^q = \alpha$ for all $\alpha \in \mathbb{F}_q$.

The following two theorems tells us why we care about the Frobenius.

Theorem. Consider $\mathbb{F}_{q^n}/\mathbb{F}_q$. Then Fr_q is an element of order n as an element of $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$.

Proof. For all $\alpha \in \mathbb{F}_{q^n}$, we have $\mathrm{Fr}_q^n(\alpha) = \alpha^{q^n} = \alpha$. So the order of Fr_q divides n.

If $m \mid n$, then the set

$$\{\alpha \in \mathbb{F}_{q^n} : \mathrm{Fr}_q^m(\alpha) = \alpha\} = \{\alpha \in \mathbb{F}_{q^n} : \alpha^{q^m} = \alpha\} = \mathbb{F}_{q^m}.$$

So if m is the order of Fr_q, then $\mathbb{F}_{q^m} = \mathbb{F}_{q^n}$. So $m = n$. □

Theorem. The extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois with Galois group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n}) \cong \mathbb{Z}/n\mathbb{Z}$, generated by Fr_q.

Proof. The multiplicative group $\mathbb{F}_{q^n}^* = \mathbb{F}_{q^n} \setminus \{0\}$ is finite. We have previously seen that multiplicative groups of finite fields are cyclic. So let α be a generator of this group. Then $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. Let P_α be the minimal polynomial of α over $\mathbb{F}_q$. Then since $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ has an element of order n, we get

$$n \leq |\operatorname{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})| = |\operatorname{Hom}_{\mathbb{F}_q}(\mathbb{F}_q(\alpha), \mathbb{F}_{q^n})|.$$

Since $F_q(\alpha)$ is generated by one element, we know

$$|\operatorname{Hom}_{\mathbb{F}_q}(\mathbb{F}_q(\alpha), \mathbb{F}_{q^n})| = |\operatorname{Root}_{P_\alpha}(\mathbb{F}_{q^n})|$$

So we have

$$n \leq |\operatorname{Root}_{P_\alpha}(\mathbb{F}_{q^n})| \leq \deg P_\alpha = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n.$$

So we know that

$$|\operatorname{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})| = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n.$$

So $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a Galois extension.

Since $|\operatorname{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})|$, it has to be generated by Fr_q, since this has order n. In particular, this group is cyclic. □

We see that finite fields are rather nice — there is exactly one field of order p^d for each d and prime p, and these are all of the finite fields. All extensions are Galois and the Galois group is a simple cyclic group.

Example. Consider $\mathbb{F}_2/\mathbb{F}_2$. We can write

$$\mathbb{F}_2 = \{0, 1\} \subseteq \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\},$$

where α is a generator of $\mathbb{F}_4^*$. Define $\phi \in \mathrm{Aut}_{\mathbb{F}_2}(\mathbb{F}_4)$ by $\phi(\alpha) = \alpha^2$. Then

$$\mathrm{Aut}_{\mathbb{F}_2}(\mathbb{F}_4) = \{\mathrm{id}, \phi\}$$

since it has order 2.

Note that we can also define the Frobenius $\mathrm{Fr}_p : \bar{\mathbb{F}}_p \to \bar{\mathbb{F}}_p$, where $\alpha \mapsto \alpha^p$. Then $\mathbb{F}_{p^d}$ is the elements of $\bar{\mathbb{F}}_p$ fixed by Fr_p^d. So we can recover this subfield by just looking at the Frobenius.

3 Solutions to polynomial equations

We have now proved the fundamental theorem of Galois theory, and this gives a one-to-one correspondence between (intermediate) field extensions and subgroups of the Galois group. That is our first goal achieved. Our next big goal is to use this Galois correspondence to show that, in general, polynomials of degree 5 or more cannot be solved by radicals.

First of all, we want to make this notion of "solving by radicals" precise. We all know what this means if we are working over $\mathbb{Q}$, but we need to be very precise when working with arbitrary fields.

For example, we know that the polynomial $f = t^3 - 5 \in \mathbb{Q}[t]$ can be "solved by radicals". In this case, we have

$$\mathrm{Root}_f(\mathbb{C}) = \{\sqrt[3]{5}, \mu\sqrt[3]{5}, \mu^2\sqrt[3]{5}\},$$

where $\mu^3 = 1, \mu \neq 1$. In general fields, we want to properly define the analogues of μ and $\sqrt[3]{5}$.

These will correspond to two different concepts. The first is *cyclotomic extensions*, where the extension adds the analogues of μ, and the second is *Kummer extensions*, where we add things like $\sqrt[3]{5}$.

Then, we would say a polynomial is soluble by radicals if the splitting field of the polynomial can be obtained by repeatedly taking cyclotomic and Kummer extensions.

3.1 Cyclotomic extensions

Definition (Cyclotomic extension)**.** For a field K, we define the nth *cyclotomic extension* to be the splitting field of $t^n - 1$.

Note that if K is a field and L is the nth cyclotomic extension, then $\mathrm{Root}_{t^n-1}(L)$ is a subgroup of multiplicative group $L^* = L \setminus \{0\}$. Since this is a finite subgroup of L^*, it is a cyclic group.

Moreover, if $\mathrm{char}\, K = 0$ or $0 < \mathrm{char}\, K \nmid n$, then $(t^n - 1)' = nt^{n-1}$ and this has no common roots with $t^n - 1$. So $t^n - 1$ has no repeated roots. In other words, $t^n - 1$ has n distinct roots. So as a group,

$$\mathrm{Root}_{t^n-1}(L) \cong \mathbb{Z}/n\mathbb{Z}.$$

In particular, this group has at least one element μ of order n.

Definition (Primitive root of unity)**.** The *nth primitive root of unity* is an element of order n in $\mathrm{Root}_{t^n-1}(L)$.

These elements correspond to the elements of the multiplicative group of units in $\mathbb{Z}/n\mathbb{Z}$, written $(\mathbb{Z}/n\mathbb{Z})^\times$.

The next theorem tells us some interesting information about these roots and some related polynomials.

Theorem. For each $d \in \mathbb{N}$, there exists a *dth cyclotomic monic polynomial* $\phi_d \in \mathbb{Z}[t]$ satisfying:

(i) For each $n \in \mathbb{N}$, we have

$$t^n - 1 = \prod_{d|n} \phi_d.$$

(ii) Assume $\operatorname{char} K = 0$ or $0 < \operatorname{char} K \nmid n$. Then

$$\operatorname{Root}_{\phi_n}(L) = \{n\text{th primitive roots of unity}\}.$$

Note that here we have an abuse of notation, since ϕ_n is a polynomial in $\mathbb{Z}[t]$, not $K[t]$, but we can just use the canonical map $\mathbb{Z}[t] \to K[t]$ mapping 1 to 1 and t to t.

Proof. We do induction on n to construct ϕ_n. When $n = 1$, let $\phi_1 = t - 1$. Then (i) and (ii) hold in this case, trivially.

Assume now that (i) and (ii) hold for smaller values of n. Let

$$f = \prod_{d|n, d<n} \phi_d.$$

By induction, $f \in \mathbb{Z}[t]$. Moreover, if $d \mid n$ and $d < n$, then $\phi_d \mid (t^n - 1)$ because $(t^d - 1) \mid (t^n - 1)$. We would like to say that f also divides $t^n - 1$. However, we have to be careful, since to make this conclusion, we need to show that ϕ_d and $\phi_{d'}$ have no common roots for distinct $d, d' \mid n$ (and $d, , d' < n$).

Indeed, by induction, ϕ_d and ϕ_d' have no common roots because

$$\operatorname{Root}_{\phi_d}(L) = \{d\text{th primitive roots of unity}\},$$
$$\operatorname{Root}_{\phi_{d'}}(L) = \{d'\text{th primitive roots of unity}\},$$

and these two sets are disjoint (or else the roots would not be *primitive*). Therefore ϕ_d and $\phi_{d'}$ have no common irreducible factors. Hence $f \mid t^n - 1$. So we can write

$$t^n - 1 = f\phi_n,$$

where $\phi_n \in \mathbb{Q}[t]$. Since f is monic, ϕ_n has integer coefficients. So indeed $\phi_n \in \mathbb{Z}[t]$. So the first part is proven.

To prove the second part, note that by induction,

$$\operatorname{Root}_f(L) = \{\text{non-primitive } n\text{th roots of unit}\},$$

since all nth roots of unity are dth primitive roots of unity for some smaller d.

Since $f\phi_n = t^n - 1$, ϕ_n contains the remaining, primitive nth roots of unit. Since $t^n - 1$ has no repeated roots, we know that ϕ_n does not contain any extra roots. So

$$\operatorname{Root}_{\phi_n}(L) = \{n\text{th primitive roots of unity}\}. \qquad \square$$

These ϕ_n are what we use to "build up" the polynomials $t^n - 1$. These will later serve as a technical tool to characterize the Galois group of the nth cyclotomic extension of $\mathbb{Q}$.

Before we an reach that, we first take a tiny step, and prove something that works for arbitrary fields first.

Theorem. Let K be a field with $\operatorname{char} K = 0$ or $0 < \operatorname{char} K \nmid n$. Let L be the nth cyclotomic extension of K. Then L/K is a Galois extension, and there is an injective homomorphism $\theta : \operatorname{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$.

In addition, every irreducible factor of ϕ_n (in $K[t]$) has degree $[L : K]$.

The important thing about our theorem is the homomorphism

$$\theta : \mathrm{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times.$$

In general, we don't necessarily know much about $\mathrm{Gal}(L/K)$, but the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is well-understood. In particular, we now know that $\mathrm{Gal}(L/K)$ is abelian.

Proof. Let μ be an nth primitive root of unity. Then

$$\mathrm{Root}_{t^n-1}(L) = \{1, \mu, \mu^2, \cdots, \mu^{n-1}\}$$

is a cyclic group of order n generated by μ. We first construct the homomorphism $\theta : \mathrm{Aut}_K(L) \to (\mathbb{Z}/n\mathbb{Z})^\times$ as follows: for each $\phi \in \mathrm{Aut}_K(L)$, ϕ is completely determined by the value of $\phi(\mu)$ since $L = K(\mu)$. Since ϕ is an automorphism, it must take an nth primitive root of unity to another nth primitive root of unity. So $\phi(\mu) = \mu^i$ for some i such that $(i, n) = 1$. Now let $\theta(\phi) = \bar{i} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Note that this is well-defined since if $\mu^i = \mu^j$, then $i - j$ has to be a multiple of n.

Now it is easy to see that if $\phi, \psi \in \mathrm{Aut}_K(L)$ are given by $\phi(\mu) = \mu^i$, and $\psi(\mu) = \mu^j$, then $\phi \circ \psi(\mu) = \phi(\mu^j) = \mu^{ij}$. So $\theta(\phi\psi) = \bar{ij} = \theta(\phi)\theta(\psi)$. So θ is a group homomorphism.

Now we check that θ is injective. If $\theta(\phi) = \bar{1}$ (note that $(\mathbb{Z}/n\mathbb{Z})^\times$ is a multiplicative group with unit 1), then $\phi(\mu) = \mu$. So $\phi = \mathrm{id}$.

Now we show that L/K is Galois. Recall that $L = K(\mu)$, and let P_μ be a minimal polynomial of μ over K. Since μ is a root of $t^n - 1$, we know that $P_\mu \mid t^n - 1$. Since $t^n - 1$ has no repeated roots, P_μ has no repeated roots. So P_μ is separable. Moreover, P_μ splits over L as $t^n - 1$ splits over L. So the extension is separable and normal, and hence Galois.

Applying the previous theorem, each irreducible factor g of ϕ_n is a minimal polynomial of some nth primitive root of unity, say λ. Then $L = K(\lambda)$. So

$$\deg g = \deg P_\lambda = [K(\lambda) : K] = [L : K]. \qquad \square$$

Example. We can calculate the following in $\mathbb{Q}[t]$.

(i) $\phi_1 = t - 1$.

(ii) $\phi_2 = t + 1$ since $t^2 - 1 = \phi_1\phi_2$.

(iii) $\phi_3 = t^2 + t + 1$.

(iv) $\phi_4 = t^2 + 1$.

These are rather expected. Now take $K = \mathbb{F}_2$. Then $1 = -1$. So we might be able to further decompose these polynomials. For example, $t + 1 = t - 1$ in $\mathbb{F}_2$. So we have

$$\phi_4 = t^2 + 1 = t^2 - 1 = \phi_1\phi_2.$$

So in $\mathbb{F}_2$, ϕ_4 is not irreducible. Similarly, if we have too much time, we can show that

$$\phi_{15} = (t^4 + t + 1)(t^4 + t^3 + 1).$$

So ϕ_{15} is not irreducible. However, they *are* irreducible over the rationals, as we will soon see.

So far, we know $\mathrm{Gal}(L/K)$ is an abelian group, isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. However, we are greedy and we want to know more. The following lemma tells us when this θ is an isomorphism.

Lemma. Under the notation and assumptions of the previous theorem, ϕ_n is irreducible in $K[t]$ if and only if θ is an isomorphism.

Proof. ($\Rightarrow$) Suppose ϕ_n is irreducible. Recall that $\mathrm{Root}_{\phi_n}(L)$ is exactly the nth primitive roots of unity. So if μ is an nth primitive root of unity, then P_μ, the minimal polynomial of μ over K is ϕ_n. In particular, if λ is also an nth primitive root of unity, then $P_\mu = P_\lambda$. This implies that there is some $\phi_\lambda \in \mathrm{Aut}_K(L)$ such that $\phi_\lambda(\mu) = \lambda$.

Now if $\bar{i} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then taking $\lambda = \mu^i$, this shows that we have $\phi_\lambda \in \mathrm{Aut}_K(L)$ such that $\theta(\phi_\lambda) = \bar{i}$. So θ is surjective, and hence an isomorphism.

($\Leftrightarrow$) Suppose that θ is an isomorphism. We will reverse the above argument and show that all roots have the same minimal polynomial. Let μ be a nth primitive root of unity, and pick $\bar{i} \in (\mathbb{Z}/n\mathbb{Z})^\times$, and let $\lambda = \mu^i$. Since θ is an isomorphism, there is some $\phi_\lambda \in \mathrm{Aut}_K(L)$ such that $\theta(\phi_\lambda) = \bar{i}$, i.e. $\phi_\lambda(\mu) = \mu^i = \lambda$. Then we must have $P_\mu = P_\lambda$.

Since every nth primitive root of unity is of the form μ^i (with $(i, n) = 1$), this implies that all nth primitive roots have the same minimal polynomial. Since the roots of ϕ_n are all the nth primitive roots of unity, its irreducible factors are exactly the minimal polynomials of the primitive roots. Moreover, ϕ_n does not have repeated roots. So $\phi_n = P_\mu$. In particular, ϕ_n is irreducible. □

We want to apply this lemma to the case of rational numbers. We want to show that θ is an isomorphism. So we have to show that ϕ_n is irreducible in $\mathbb{Q}[t]$.

Theorem. ϕ_n is irreducible in $\mathbb{Q}[t]$. In particular, it is also irreducible in $\mathbb{Z}[t]$.

Proof. As before, this can be achieved by showing that all nth primitive roots have the same minimal polynomial. Moreover, let μ be our favorite nth primitive root. Then all other primitive roots λ are of the form $\lambda = \mu^i$, where $(i, n) = 1$. By the fundamental theorem of arithmetic, we can write i as a product $i = q_1 \cdots q_n$. Hence it suffices to show that for all primes $q \nmid n$, we have $P_\mu = P_{\mu^q}$. Noting that μ^q is also an nth primitive root, this gives

$$P_\mu = P_{\mu^{q_1}} = P_{(\mu^{q_1})^{q_2}} = P_{\mu^{q_1 q_2}} = \cdots = P_{\mu^{q_1 \cdots q_r}} = P_{\mu^i}.$$

So we now let μ be an nth primitive root, P_μ be its minimal polynomial. Since μ is a root of ϕ_n, we can write $P_\mu \mid \phi_n$ inside $\mathbb{Q}[t]$. So we can write

$$\phi_n = P_\mu R,$$

Since ϕ_n and P_μ are monic, R is also monic. By Gauss' lemma, we must have $P_\mu, R \in \mathbb{Z}[t]$.

Note that showing $P_\mu = P_{\mu^q}$ is the same as showing μ^q is a root of P_μ, since $\deg P_\mu = \deg P_{\mu^q}$. So suppose it's not. Since μ^q is an nth primitive root of unity, it is a root of ϕ_n. So μ^q must be a root of R. Now let $S = R(t^q)$. Then μ is a root of S, and so $P_\mu \mid S$.

We now reduce mod q. For any polynomial $f \in \mathbb{Z}[t]$, we write the result of reducing the coefficients mod q as $\bar{f}$. Then we have $\bar{S} = \overline{R(t^q)} = \overline{R(t)}^q$. Since

$\bar{P}_\mu$ divides $\bar{S}$ (by Gauss' lemma), we know $\bar{P}_\mu$ and $\overline{R(t)}$ have common roots. But $\bar{\phi}_n = \bar{P}_\mu \bar{R}$, and so this implies $\bar{\phi}_n$ has repeated roots. This is impossible since $\bar{\phi}^n$ divides $t^n - 1$, and since $q \nmid n$, we know the derivative of $t^n - 1$ does not vanish at the roots. So we are done. □

Corollary. Let $K = \mathbb{Q}$ and L be the nth cyclotomic extension of $\mathbb{Q}$. Then the injection $\theta : \mathrm{Gal}(L/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism.

Example. Let p be a prime number, and $q = p^d$, $d \in \mathbb{N}$. Consider $\mathbb{F}_q$, a field with q elements, and let L be the nth cyclotomic extension of $\mathbb{F}_q$ (where $p \nmid n$). Then we have a homomorphism $\theta : \mathrm{Gal}(L/\mathbb{F}_q) \to (\mathbb{Z}/n\mathbb{Z})^\times$.

We have previously shown that $\mathrm{Gal}(L/\mathbb{F}_q)$ must be a cyclic group. So if $(\mathbb{Z}/n\mathbb{Z})^\times$ is non-cyclic, then θ is not an isomorphism, and ϕ_n is not irreducible in $\mathbb{F}_q[t]$.

For example, take $p = q = 7$ and $n = 8$. Then

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$$

is not cyclic, because manual checking shows that there is no element of order 4. Hence $\theta : \mathrm{Gal}(L/\mathbb{F}_7) \to (\mathbb{Z}/8\mathbb{Z})^\times$ is not an isomorphism, and ϕ_8 is not irreducible in $\mathbb{F}_7[t]$.

3.2 Kummer extensions

We shall now consider a more general case, and study the splitting field of $t^n - \lambda \in K[t]$. As we have previously seen, we will need to make use of the nth primitive roots of unity.

The definition of a Kummer extension will involve a bit more that it being the splitting field of $t^n - \lambda$. So before we reach the definition, we first studying some properties of an arbitrary splitting field of $t^n - \lambda$, and use this to motivate the definition of a Kummer extension.

Definition (Cyclic extension)**.** We say a Galois extension L/K is *cyclic* is $\mathrm{Gal}(L/K)$ is a cyclic group.

Theorem. Let K be a field, $\lambda \in K$ non-zero, $n \in \mathbb{N}$, $\mathrm{char}\, K = 0$ or $0 < \mathrm{char}\, K \nmid n$. Let L be the splitting field of $t^n - \lambda$. Then

(i) L contains an nth primitive root of unity, say μ.

(ii) $L/K(\mu)$ is a cyclic (and in particular Galois) extension with degree $[L : K(\mu)] \mid n$.

(iii) $[L : K(\mu)] = n$ if and only if $t^n - \lambda$ is irreducible in $K(\mu)[t]$.

Proof.

(i) Under our assumptions, $t^n - \lambda$ and $(t^n - \lambda)' = nt^{n-1}$ have no common roots in L. So $t^n - \lambda$ has distinct roots in L, say $\alpha_1, \cdots, \alpha_n \in L$.

It then follows by direct computation that $\alpha_1\alpha_1^{-1}, \alpha_2\alpha_1^{-1}, \cdots, \alpha_n\alpha_1^{-1}$ are distinct roots of unity, i.e. roots of $t^n - 1$. Then one of these, say μ must be an nth primitive root of unity.

(ii) We know $L/K(\mu)$ is a Galois extension because it is the splitting field of the separable polynomial $t^n - \lambda$.

To understand the Galois group, we need to know how this field exactly looks like. We let α be any root of $t^n - \lambda$. Then the set of all roots can be written as

$$\{\alpha, \mu\alpha, \mu^2\alpha, \cdots, \mu^{n-1}\alpha\}$$

Then

$$L = K(\alpha_1, \cdots, \alpha_n) = K(\mu, \alpha) = K(\mu)(\alpha).$$

Thus, any element of $\mathrm{Gal}(L/K(\mu))$ is uniquely determined by what it sends α to, and any homomorphism must send α to one of the other roots of $t^n - \lambda$, namely $\mu^i\alpha$ for some i.

Define a homomorphism $\sigma : \mathrm{Gal}(L/K(\mu)) \to \mathbb{Z}/n\mathbb{Z}$ that sends ϕ to the corresponding i (as an element of $\mathbb{Z}/n\mathbb{Z}$, so that it is well-defined).

It is easy to see that σ is an injective group homomorphism. So we know $\mathrm{Gal}(L/K(\mu))$ is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$. Since the subgroup of any cyclic group is cyclic, we know that $\mathrm{Gal}(L/K(\mu))$ is cyclic, and its size is a factor of n by Lagrange's theorem. Since $|\mathrm{Gal}(L/K(\mu))| = [L : K(\mu)]$ by definition of a Galois extension, it follows that $[L : K(\mu)]$ divides n.

(iii) We know that $[L : K(\mu)] = [K(\mu, \alpha) : K(\mu)] = \deg q_\alpha$. So $[L : K(\mu)] = n$ if and only if $\deg q_\alpha = n$. Since q_α is a factor of $t^n - \lambda$, $\deg q_\alpha = n$ if and only if $q_\alpha = t^n - \lambda$. This is true if and only if $t^n - \lambda$ is irreducible $K(\mu)[t]$. So done. □

Example. Consider $t^4 + 2 \in \mathbb{Q}[t]$. Let $\mu = \sqrt{-1}$, which is a 4th primitive root of unity. Now

$$t^4 + 2 = (t - \alpha)(t + \alpha)(t - \mu\alpha)(t + \mu\alpha),$$

where $\alpha = \sqrt[4]{-2}$ is one of the roots of $t^4 + 2$. Then we have the field extension $\mathbb{Q} \subseteq \mathbb{Q}(\mu) \subseteq \mathbb{Q}(\mu, \alpha)$, where $\mathbb{Q}(\mu, \alpha)$ is a splitting field of $t^4 + 2$.

Since $\sqrt{-2} \notin \mathbb{Q}(\mu)$, we know that $t^4 + 2$ is irreducible in $\mathbb{Q}(\mu)[t]$ by looking at the factorization above. So by our theorem, $\mathbb{Q}(\mu) \subseteq \mathbb{Q}(\mu, \alpha)$ is a cyclic extension of degree exactly 4.

Definition (Kummer extension)**.** Let K be a field, $\lambda \in K$ non-zero, $n \in \mathbb{N}$, $\mathrm{char}\, K = 0$ or $0 < \mathrm{char}\, K \nmid n$. Suppose K contains an nth primitive root of unity, and L is a splitting field of $t^n - \lambda$. If $\deg[L : K] = n$, we say L/K is a *Kummer extension.*

Note that we used to have extensions $K \subseteq K(\mu) \subseteq L$. But if K already contains a primitive root of unity, then $K = K(\mu)$. So we are left with the cyclic extension $K \subseteq L$.

To following technical lemma will be useful:

Lemma. Assume L/K is a field extension. Then $\mathrm{Hom}_K(L, L)$ is linearly independent. More concretely, let $\lambda_1, \cdots, \lambda_n \in L$ and $\phi_1, \cdots, \phi_n \in \mathrm{Hom}_K(L, L)$ distinct. Suppose for all $\alpha \in L$, we have

$$\lambda_1\phi_1(\alpha) + \cdots + \lambda_n\phi_n(\alpha) = 0.$$

Then $\lambda_i = 0$ for all i.

Proof. We perform induction on n.

Suppose we have some $\lambda_i \in L$ and $\phi_i \in \mathrm{Hom}_K(L, L)$ such that

$$\lambda_1\phi_1(\alpha) + \cdots + \lambda_n\phi_n(\alpha) = 0.$$

The $n = 1$ case is trivial, since $\lambda_1\phi_1 = 0$ implies $\lambda_1 = 0$ (the zero homomorphism does not fix K).

Otherwise, since the homomorphisms are distinct, pick $\beta \in L$ such that $\phi_1(\beta) \neq \phi_n(\beta)$. Then we know that

$$\lambda_1\phi_1(\alpha\beta) + \cdots + \lambda_n\phi_n(\alpha\beta) = 0$$

for all $\alpha \in L$. Since ϕ_i are homomorphisms, we can write this as

$$\lambda_1\phi_1(\alpha)\phi_1(\beta) + \cdots + \lambda_n\phi_n(\alpha)\phi_n(\beta) = 0.$$

On the other hand, by just multiplying the original equation by $\phi_n(\beta)$, we get

$$\lambda_1\phi_1(\alpha)\phi_n(\beta) + \cdots + \lambda_n\phi_n(\alpha)\phi_n(\beta) = 0.$$

Subtracting the equations gives

$$\lambda_1\phi_1(\alpha)(\phi_1(\beta) - \phi_n(\beta)) + \cdots + \lambda_{n-1}\phi_{n-1}(\alpha)(\phi_{n-1}(\beta) - \phi_n(\beta)) = 0$$

for all $\alpha \in L$. By induction, $\lambda_i(\phi_i(\beta) - \phi_n(\beta)) = 0$ for all $1 \leq i \leq n-1$. In particular, since $\phi_1(\beta) - \phi_n(\beta) \neq 0$, we have $\lambda_1 = 0$. Then we are left with

$$\lambda_2\phi_2(\alpha) + \cdots + \lambda_n\phi_n(\alpha) = 0.$$

Then by induction again, we know that all coefficients are zero. □

Theorem. Let K be a field, $n \in \mathbb{N}$, $\mathrm{char}\, K = 0$ or $0 < \mathrm{char}\, K \nmid n$. Suppose K contains an nth primitive root of unity, and L/K is a cyclic extension of degree $[L : K] = n$. Then L/K is a Kummer extension.

This is a rather useful result. If we look at the splitting field of a polynomial $t^n - \lambda$, even if the ground field includes the right roots of unity, *a priori*, this doesn't have to be a Kummer extension if it doesn't have degree n. But we previously showed that the extension must be cyclic. And so this theorem shows that it is still a Kummer extension of some sort.

This is perhaps not too surprising. For example, if, say, $n = 4$ and λ is secretly a square, then the splitting field of $t^4 - \lambda$ is just the splitting field of $t^2 - \sqrt{\lambda}$.

Proof. Our objective here is to find a clever $\lambda \in K$ such that L is the splitting field of $t^n - \lambda$. To do so, we will have to hunt for a root β of $t^n - \lambda$ in L.

Pick ϕ a generator of $\mathrm{Gal}(L/K)$. We know that if β were a root of $t^n - \lambda$, then $\phi(\beta) = \mu^{-1}\beta$ for some primitive nth root of unity μ. Thus, we want to find an element that satisfies such a property.

By the previous lemma, we can find some $\alpha \in L$ such that

$$\beta = \alpha + \mu\phi(\alpha) + \mu^2\phi^2(\alpha) + \cdots + \mu^{n-1}\phi^{n-1}(\alpha) \neq 0.$$

Then, noting that ϕ^n is the identity and ϕ fixes $\mu \in K$, we see that β trivially satisfies

$$\phi(\beta) = \phi(\alpha) + \mu\phi^2\alpha + \cdots + \mu^{n-1}\phi^n(\alpha) = \mu^{-1}\beta,$$

In particular, we know that $\phi(\beta) \in K(\beta)$.

Now pick $\lambda = \beta^n$. Then $\phi(\beta^n) = \mu^{-n}\beta^n = \beta^n$. So ϕ fixes β^n. Since ϕ generates $\mathrm{Gal}(L/K)$, we know all automorphisms of L/K fixes β^n. So $\beta^n \in K$.

Now the roots of $t^n - \lambda$ are $\beta, \mu\beta, \cdots, \mu^{n-1}\beta$. Since these are all in β, we know $K(\beta)$ is the splitting field of $t^n - \lambda$.

Finally, to show that $K(\beta) = L$, we observe that $\mathrm{id}, \phi|_{K(\beta)}, \ldots, \phi^n|_{K(\beta)}$ are distinct elements of $\mathrm{Aut}_K(K(\beta))$ since they do different things to β. Recall our previous theorem that

$$[K(\beta) : K] \geq |\mathrm{Aut}_K(K(\beta))|.$$

So we know that $n = [L : K] = [K(\beta) : K]$. So $L = K(\beta)$. So done. □

Example. Consider $t^3 - 2 \in \mathbb{Q}[t]$, and μ a third primitive root of unity. Then we have the extension $\mathbb{Q} \subseteq \mathbb{Q}(\mu) \subseteq \mathbb{Q}(\mu, \sqrt[3]{2})$. Then $\mathbb{Q} \subseteq \mathbb{Q}(\mu)$ is a cyclotomic extension of degree 2, and $\mathbb{Q}(\mu) \subseteq \mathbb{Q}(\mu, \sqrt[3]{2})$ is a Kummer extension of degree 3.

3.3 Radical extensions

We are going to put these together and look at radical extensions, which allows us to characterize what it means to "solve a polynomial with radicals".

Definition (Radical extension)**.** A field extension L/K is *radical* if there is some further extension E/L and with a sequence

$$K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_r = E,$$

such that each $E_i \subseteq E_{i+1}$ is a cyclotomic or Kummer extension, i.e. E_{i+1} is a splitting field of $t^n - \lambda_{i+1}$ over E_i for some $\lambda_{i+1} \in E_i$.

Informally, we say E_{i+1} is obtained by adding the roots "$\sqrt[n]{\lambda_{i+1}}$" to E_i. Hence we interpret a radical extension as an extension that only adds radicals.

Definition (Solubility by radicals)**.** Let K be a field, and $f \in K[t]$. f. We say f is *soluble by radicals* if the splitting field of f is a radical extension of K.

This means that f can be solved by radicals of the form $\sqrt[n]{\lambda_i}$.

Let's go back to our first lecture and describe what we've done in the language we've developed in the course.

Example. As we have shown in lecture 1, any polynomial $f \in \mathbb{Q}[t]$ of degree at most 4 can be solved by radicals.

For example, assume $\deg f = 3$. So $f = t^3 + at^2 + bt + c$. Let L be the splitting field of f. Recall we reduced the problem of "solving" f to the case $a = 0$ by the substitution $x \mapsto x - \frac{a}{3}$. Then we found our $\beta, \gamma \in \mathbb{C}$ such that each root α_i can be written as a linear combination of β and γ (and μ), i.e. $L \subseteq \mathbb{Q}(\beta, \gamma, \mu)$.

Then we showed that

$$\{\beta^3, \gamma^3\} = \left\{ \frac{-27c \pm \sqrt{(27c)^2 + 4 \times 27b^3}}{2} \right\}.$$

We now let

$$\lambda = \sqrt{(27c)^2 + 4 \times 27b^3}.$$

Then we have the extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\lambda) \subseteq \mathbb{Q}(\lambda, \mu) \subseteq \mathbb{Q}(\lambda, \mu, \beta),$$

and also

$$\mathbb{Q} \subseteq L \subseteq \mathbb{Q}(\lambda, \mu, \beta).$$

Note that the first extension $\mathbb{Q} \subseteq \mathbb{Q}(\lambda)$ is a Kummer extension since it is a splitting field of $t^2 - \lambda^2$. Then $\mathbb{Q}(\lambda) \subseteq \mathbb{Q}(\lambda, \mu)$ is the third cyclotomic extension. Finally, $\mathbb{Q}(\lambda, \mu) \subseteq \mathbb{Q}(\lambda, \mu\beta)$ is a Kummer extension, the splitting field of $t^3 - \beta^3$. So $\mathbb{Q} \subseteq L$ is a radical extension.

Let's go back to the definition of a radical extension. We said L/K is radical if there is a further extension E/L that satisfies certain nice properties. It would be great if E/K is actually a Galois extensions. To show this, we first need a technical lemma.

Lemma. Let L/K be a Galois extension, $\operatorname{char} K = 0$, $\gamma \in L$ and F the splitting field of $t^n - \gamma$ over L. Then there exists a further extension E/F such that E/L is radical and E/K is Galois.

Here we have the inclusions

$$K \subseteq L \subseteq F \subseteq E,$$

where K, L and F are given and E is what we need to find. The idea of the proof is that we just add in the "missing roots" to obtain E so that E/K is Galois, and doing so only requires performing cyclotomic and Kummer extensions.

Proof. Since we know that L/K is Galois, we would rather work in K than in L. However, our γ is in L, not K. Hence we will employ a trick we've used before, where we introduce a new polynomial f, and show that its coefficients are fixed by $\operatorname{Gal}(L/K)$, and hence in K. Then we can look at the splitting field of f or its close relatives.

Let

$$f = \prod_{\phi \in \operatorname{Gal}(L/K)} (t^n - \phi(\gamma)).$$

Each $\phi \in \operatorname{Gal}(L/K)$ induces a homomorphism $L[t] \to L[t]$. Since each $\phi \in \operatorname{Gal}(L/K)$ just rotates the roots of f around, we know that this induced homomorphism fixes f. Since all automorphisms in $\operatorname{Gal}(L/K)$ fix the coefficients of f, the coefficients must all be in K. So $f \in K[t]$.

Now since L/K is Galois, we know that L/K is normal. So L is the splitting field of some $g \in K[t]$. Let E be the splitting field of fg over K. Then $K \subseteq E$ is normal. Since the characteristic is zero, this is automatically separable. So the extension $K \subseteq E$ is Galois.

We have to show that $L \subseteq E$ is a radical extension. We pick our fields as follows:

- $E_0 = L$
- $E_1 =$ splitting field of $t^n - 1$ over E_0

- E_2 = splitting field of $t^n - \gamma$ over E_1
- E_3 = splitting field of $t^n - \phi_1(\gamma)$ over E_2
- $\cdots$
- $E_r = E$,

where we enumerate $\mathrm{Gal}(L/K)$ as $\{\mathrm{id}, \phi_1, \phi_2, \cdots\}$.

We then have the sequence of extensions

$$L = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_r$$

Here $E_0 \subseteq E_1$ is a cyclotomic extension, and $E_1 \subseteq E_2$, $E_2 \subseteq E_3$ etc. are Kummer extensions since they contain enough roots of unity and are cyclic. By construction, $F \subseteq E_2$. So $F \subseteq E$. □

Theorem. Suppose L/K is a radical extension and $\mathrm{char}\, K = 0$. Then there is an extension E/L such that E/K is Galois and there is a sequence

$$K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E,$$

where $E_i \subseteq E_{i+1}$ is cyclotomic or Kummer.

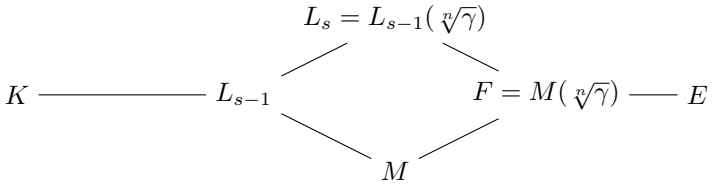
Proof. Note that this is equivalent to proving the following statement: Let

$$K = L_0 \subseteq L_1 \subseteq \cdots L_s$$

be a sequence of cyclotomic or Kummer extensions. Then there exists an extension $L_s \subseteq E$ such that $K \subseteq E$ is Galois and can be written as a sequence of cyclotomic or Kummer extensions.

We perform induction on s. The $s = 0$ case is trivial.

If $s > 0$, then by induction, there is an extension M/L_{s-1} such that M/K is Galois and is a sequence of cyclotomic and Kummer extensions. Now L_s is a splitting field of $t^n - \gamma$ over L_{s-1} for some $\gamma \in L_{s-1}$. Let F be the splitting field of $t^n - \gamma$ over M. Then by the lemma and its proof, there exists an extension E/M that is a sequence of cyclotomic or Kummer extensions, and E/K is Galois.



However, we already know that M/K is a sequence of cyclotomic and Kummer extensions. So E/K is a sequence of cyclotomic and Kummer extension. So done. □

3.4 Solubility of groups, extensions and polynomials

Let $f \in K[t]$. We defined the notion of solubility of f in terms of radical extensions. However, can we decide whether f is soluble or not without resorting to the definition? In particular, is it possible to decide whether its soluble by just looking at $\mathrm{Gal}(L/K)$, where L is the splitting field of f over K? It would be great if we could do so, since groups are easier to understand than fields.

The answer is yes. It turns out the solubility of f corresponds to the solubility of $\mathrm{Gal}(L/K)$. Of course, we will have to first define what it means for a group to be soluble. After that, we will find examples of polynomials f of degree at least 5 such that $\mathrm{Gal}(L/K)$ is not soluble. In other words, there are polynomials that cannot be solved by radicals.

Definition (Soluble group)**.** A finite group G is *soluble* if there exists a sequence of subgroups

$$G_r = \{1\} \lhd \cdots \lhd G_1 \lhd G_0 = G,$$

where G_{i+1} is normal in G_i and G_i/G_{i+1} is cyclic.

Example. Any finite abelian group is solvable by the structure theorem of finite abelian groups:

$$G \cong \frac{\mathbb{Z}}{\langle n_1 \rangle} \times \cdots \times \frac{\mathbb{Z}}{\langle n_r \rangle}.$$

Example. Let S_n be the symmetric group of permutations of n letters. We know that G_3 is soluble since

$$\{1\} \lhd A_3 \lhd S_3,$$

where $S_3/A_3 \cong \mathbb{Z}/\langle 2 \rangle$ and $A_3/\{0\} \cong \mathbb{Z}/\langle 3 \rangle$.

S_4 is also soluble by

$$\{1\} \lhd \{e, (1\ 2)(3\ 4)\} \lhd \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \lhd A_4 \lhd S_4.$$

We can show that the quotients are $\mathbb{Z}/\langle 2 \rangle$, $\mathbb{Z}/\langle 3 \rangle$, $\mathbb{Z}/\langle 2 \rangle$ and $\mathbb{Z}/\langle 2 \rangle$ respectively.

How about S_n for higher n? It turns out they are no longer soluble for $n \geq 5$. To prove this, we first need a lemma.

Lemma. Let G be a finite group. Then

(i) If G is soluble, then any subgroup of G is soluble.

(ii) If $A \lhd G$ is a normal subgroup, then G is soluble if and only if A and G/A are both soluble.

Proof.

(i) If G is soluble, then by definition, there is a sequence

$$G_r = \{1\} \lhd \cdots \lhd G_1 \lhd G_0 = G,$$

such that G_{i+1} is normal in G_i and G_i/G_{i+1} is cyclic.

Let $H_i = H \cap G_i$. Note that H_{i+1} is just the kernel of the obvious homomorphism $H_i \to G_i/G_{i+1}$. So $H_{i+1} \lhd H_i$. Also, by the first isomorphism theorem, this gives an injective homomorphism $H_i/H_{i+1} \to G_i/G_{i+1}$. So H_i/H_{i+1} is cyclic. So H is soluble.

(ii) ($\Rightarrow$) By (i), we know that A is solvable. To show the quotient is soluble, by assumption, we have the sequence

$$G_r = \{1\} \lhd \cdots \lhd G_1 \lhd G_0 = G,$$

such that G_{i+1} is normal in G_i and G_i/G_{i+1} is cyclic. We construct the sequence for the quotient in the obvious way. We want to define E_i as the quotient G_i/A, but since A is not necessarily a subgroup of E, we instead define E_i to be the image of quotient map $G_i \to G/A$. Then we have a sequence

$$E_r = \{1\} \lhd \cdots \lhd E_0 = G/A.$$

The quotient map induces a surjective homomorphism $G_i/G_{i+1} \to E_i/E_{i+1}$, showing that E_i/E_{i+1} are cyclic.

($\Leftarrow$) From the assumptions, we get the sequences

$$A_m = \{1\} \lhd \cdots \lhd A_0 = A$$

$$F_n = A \lhd \cdots \lhd F_0 = G$$

where each quotient is cyclic. So we get a sequence

$$A_m = \{1\} \lhd A_1 \lhd \cdots \lhd A_0 = F_n \lhd F_{n-1} \lhd \cdots \lhd F_0 = G,$$

and each quotient is cyclic. So done. □

Example. We want to show that S_n is not soluble if $n \geq 5$. It is a well-known fact that A_n is a simple non-abelian group, i.e. it has no non-trivial subgroup. So A_n is not soluble. So S_n is not soluble.

The key observation in Galois theory is that solubility of polynomials is related to solubility of the Galois group.

Definition (Soluble extension)**.** A finite field extension L/K is soluble if there is some extension $L \subseteq E$ such that $K \subseteq E$ is Galois and $\mathrm{Gal}(E/K)$ is soluble.

Note that this definition is rather like the definition of a radical extension, since we do not require the extension itself to be "nice", but just for there to be a further extension that is nice. In fact, we will soon see they are the same.

Lemma. Let L/K be a Galois extension. Then L/K is soluble if and only if $\mathrm{Gal}(L/K)$ is soluble.

This means that the whole purpose of extending to E is just to make it a Galois group, and it isn't used to introduce extra solubility.

Proof. ($\Leftarrow$) is clear from definition.

($\Rightarrow$) By definition, there is some $E \subseteq L$ such that E/K is Galois and $\mathrm{Gal}(E/K)$ is soluble. By the fundamental theorem of Galois theory, $\mathrm{Gal}(L/K)$ is a quotient of $\mathrm{Gal}(E/K)$. So by our previous lemma, $\mathrm{Gal}(L/K)$ is also soluble. □

We now come to the main result of the lecture:

Theorem. Let K be a field with $\mathrm{char}\, K = 0$, and L/K is a radical extension. Then L/K is a soluble extension.

Proof. We have already shown that if we have a radical extension L/K, then there is a finite extension $K \subseteq E$ such that $K \subseteq E$ is a Galois extension, and there is a sequence of cyclotomic or Kummer extensions

$$E_0 = K \subseteq E_1 \subseteq \cdots \subseteq E_r = E.$$

Let $G_i = \mathrm{Gal}(E/E_i)$. By the fundamental theorem of Galois theory, inclusion of subfields induces an inclusion of subgroups

$$G_0 = \mathrm{Gal}(E/K) \geq G_1 \geq \cdots \geq G_r = \{1\}.$$

In fact, $G_i \rhd G_{i+1}$ because $E_i \subseteq E_{i+1}$ are Galois (since cyclotomic and Kummer extensions are). So in fact we have

$$G_0 = \mathrm{Gal}(E/K) \rhd G_1 \rhd \cdots \rhd G_r = \{1\}.$$

Finally, note that by the fundamental theorem of Galois theory,

$$G_i/G_{i+1} = \mathrm{Gal}(E_{i+1}/E_i).$$

We also know that the Galois groups of cyclotomic and Kummer extensions are abelian. Since abelian groups are soluble, our previous lemma implies that L/K is soluble. □

In fact, we will later show that the converse is also true. So an extension is soluble if and only if it is radical.

Corollary. Let K be a field with $\mathrm{char}\, K = 0$, and $f \in K[t]$. If f can be solved by radicals, then $\mathrm{Gal}(L/K)$ is soluble, where L is the splitting field of f over K.

Again, we will later show that the converse is also true. However, to construct polynomials that cannot be solved by radicals, this suffices. In fact, this corollary is all we really need.

Proof. We have seen that L/K is a Galois extension. By assumption, L/K is thus a radical extension. By the theorem, L/K is also a soluble extension. So $\mathrm{Gal}(L/K)$ is soluble. □

To find an $f \in \mathbb{Q}[t]$ which cannot be solved by radicals, it suffices to find an f such that the Galois group is not soluble. We don't know many non-soluble groups so far. So in fact, we will find an f such that $\mathrm{Gal}(L/\mathbb{Q}) = S_5$.

To do so, we want to relate Galois groups to permutation groups.

Lemma. Let K be a field, $f \in K[t]$ of degree n with no repeated roots. Let L be the splitting field of f over K. Then L/K is Galois and there exist an injective group homomorphism

$$\mathrm{Gal}(L/K) \to S_n.$$

Proof. Let $\mathrm{Root}_f(L) = \{\alpha_1, \cdots, \alpha_n\}$. Let P_{α_i} be the minimal polynomial of α_i over K. Then $P_{\alpha_i} \mid f$ implies that P_{α_i} is separable and splits over L. So L/K is Galois.

Now each $\phi \in \mathrm{Gal}(L/K)$ permutes the α_i, which gives a map $\mathrm{Gal}(L/K) \to S_n$. It is easy to show this is an injective group homomorphism. □

Note that there is not a unique or naturally-defined injective group homomorphism to S_n. This homomorphism, obviously, depends on how we decide to number our roots.

Example. Let $f = (t^2 - 2)(t^2 - 3) \in \mathbb{Q}[t]$. Let L be the splitting field of f over $\mathbb{Q}$. Then the roots are

$$\mathrm{Root}_f(L) = \{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}\}.$$

We label these roots as $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ in order. Now note that $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and thus $[L : \mathbb{Q}] = 4$. Hence $|\operatorname{Gal}(L/\mathbb{Q})| = 4$ as well. We can let $\operatorname{Gal}(L/\mathbb{Q}) = \{\mathrm{id}, \varphi, \psi, \lambda\}$, where

$$\begin{aligned} \mathrm{id}(\sqrt{2}) &= \sqrt{2} & \mathrm{id}(\sqrt{3}) &= \sqrt{3} \\ \varphi(\sqrt{2}) &= -\sqrt{2} & \varphi(\sqrt{3}) &= \sqrt{3} \\ \psi(\sqrt{2}) &= \sqrt{2} & \psi(\sqrt{3}) &= -\sqrt{3} \\ \lambda(\sqrt{2}) &= -\sqrt{2} & \lambda(\sqrt{3}) &= -\sqrt{3} \end{aligned}$$

Then the image of $\operatorname{Gal}(L/\mathbb{Q}) \to S_4$ is given by

$$\{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}.$$

What we really want to know is if there are polynomials in which this map is in fact an isomorphism, i.e. the Galois group is the symmetric group. If so, then we can use this to produce a polynomial that is not soluble by polynomials.

To find this, we first note a group-theoretic fact.

Lemma. Let p be a prime, and $\sigma \in S_p$ have order p. Then σ is a p-cycle.

Proof. By IA Groups, we can decompose σ into a product of disjoint cycles:

$$\sigma = \sigma_1 \cdots \sigma_r.$$

Let σ_i have order $m_i > 1$. Again by IA Groups, we know that

$$p = \text{order of } \sigma = \mathrm{lcm}(m_1, \cdots, m_r).$$

Since p is a prime number, we know that $p = m_i$ for all i. Hence we must have $r = 1$, since the cycles are disjoint and there are only p elements. So $\sigma = \sigma_1$. Hence σ is indeed an p cycle. □

We will use these to find an example where the Galois group is the symmetric group. The conditions for this to happen are slightly awkward, but the necessity of these will become apparent in the proof.

Theorem. Let $f \in \mathbb{Q}[t]$ be irreducible and $\deg f = p$ prime. Let $L \subseteq \mathbb{C}$ be the splitting field of f over $\mathbb{Q}$. Let

$$\mathrm{Root}_f(L) = \{\alpha_1, \alpha_2, \cdots, \alpha_{p-2}, \alpha_{p-1}, \alpha_p\}.$$

Suppose that $\alpha_1, \alpha_2, \cdots, \alpha_{p-2}$ are all real numbers, but α_{p-1} and α_p are not. In particular, $\alpha_{p-1} = \bar{\alpha}_p$. Then the homomorphism $\beta : \operatorname{Gal}(L/\mathbb{Q}) \to S_n$ is an isomorphism.

Proof. From IA groups, we know that the cycles $(1\ 2\ \cdots\ p)$ and $(p-1\ p)$ generate the whole of S_n. So we show that these two are both in the image of β.

As f is irreducible, we know that $f = P_{\alpha_1}$, the minimal polynomial of α_1 over $\mathbb{Q}$. Then

$$p = \deg P_{\alpha_i} = [\mathbb{Q}(\alpha_1) : \mathbb{Q}].$$

By the tower law, this divides $[L : \mathbb{Q}]$, which is equal to $|\operatorname{Gal}(L/\mathbb{Q})|$ since the extension is Galois. Since p divides the order of $\operatorname{Gal}(L/\mathbb{Q})$, by Cauchy's theorem of groups, there must be an element of $\operatorname{Gal}(L/\mathbb{Q})$ that is of order p. This maps to an element $\sigma \in \operatorname{im}\beta$ of order exactly p. So σ is a p-cycle.

On the other hand, the isomorphism $\mathbb{C} \to \mathbb{C}$ given by $z \mapsto \bar{z}$ restricted to L gives an automorphism in $\operatorname{Gal}(L/\mathbb{Q})$. This simply permutes α_{p-1} and α_p, since it fixes the real numbers and α_{p-1} and α_p must be complex conjugate pairs. So $\tau = (p-1\ p) \in \operatorname{im}\beta$.

Now for every $1 \leq i < p$, we know that σ^i again has order p, and hence is a p-cycle. So if we change the labels of the roots $\alpha_1, \cdots, \alpha_p$ and replace σ with σ^i, and then waffle something about combinatorics, we can assume $\sigma = (1\ 2\ \cdots\ p-1\ p)$. So done. □

Example. Let $t^5 - 4t + 2 \in \mathbb{Q}[t]$. Let L be the splitting field of f over $\mathbb{Q}$.

First note that $\deg f = 5$ is a prime. Also, by Eisenstein's criterion, f is irreducible. By finding the local maximum and minimum points, we find that f has exactly three real roots. So by the theorem, there is an isomorphism $\operatorname{Gal}(L/\mathbb{Q}) \to S_5$. In other words, $\operatorname{Gal}(L/\mathbb{Q}) \cong S_5$.

We know S_5 is not a soluble group. So f cannot be solved by radicals.

After spending 19 lectures, we have found an example of a polynomial that cannot be solved by radicals. Finally.

Note that there are, of course, many examples of $f \in \mathbb{Q}[t]$ irreducible of degree at least 5 that *can* be solved by radicals, such as $f = t^5 - 2$.

3.5 Insolubility of general equations of degree 5 or more

We now want to do something more interesting. Instead of looking at a particular example, we want to say there is no general formula for solving polynomial equations of degree 5 or above. First we want to define certain helpful notions.

Definition (Field of symmetric rational functions)**.** Let K be a field, $L = K(x_1, \cdots, x_n)$, the field of rational functions over K. Then there is an injective homomorphism $S_n \to \operatorname{Aut}_K(L)$ given by permutations of x_i.

We define the *field of symmetric rational functions* $F = L^{S_n}$ to be the fixed field of S_n.

There are a few important symmetric rational functions that we care about more.

Definition (Elementary symmetric polynomials)**.** The *elementary symmetric polynomials* are $e_1, e_2, \cdots, e_n$ defined by

$$e_i = \sum_{1 \leq l_1 < l_2 < \cdots < l_i \leq n} x_{\ell_1} \cdots x_{\ell_i}.$$

It is easy to see that

$$\begin{aligned} e_1 &= x_1 + x_2 + \cdots + x_n \\ e_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\ e_n &= x_1 \cdots x_n. \end{aligned}$$

Obviously, $e_1, \cdots, e_n \in F$.

Theorem (Symmetric rational function theorem)**.** Let K be a field, $L = K(x_1, \cdots, x_n)$. Let F the field fixed by the automorphisms that permute the x_i. Then

(i) L is the splitting field of

$$f = t^n - e_1t^{n-1} + \cdots + (-1)^n e_n$$

over F.

(ii) $F = L^{S_n} \subseteq L$ is a Galois group with $\mathrm{Gal}(L/F)$ isomorphic to S_n.

(iii) $F = K(e_1, \cdots, e_n)$.

Proof.

(i) In $L[t]$, we have

$$f = (t - x_1) \cdots (t - x_n).$$

So L is the splitting field of f over F.

(ii) By Artin's lemma, L/K is Galois and $\mathrm{Gal}(L/F) \cong S_n$.

(iii) Let $E = K(e_1, \cdots, e_n)$. Clearly, $E \subseteq F$. Now $E \subseteq L$ is a Galois extension, since L is the splitting field of f over E and f has no repeated roots.

By the fundamental theorem of Galois theory, since we have the Galois extensions $E \subseteq F \subseteq L$, we have $\mathrm{Gal}(L/F) \leq \mathrm{Gal}(L/E)$. So $S_n \leq \mathrm{Gal}(L/E)$. However, we also know that $\mathrm{Gal}(L/E)$ is a subgroup of S_n, we must have $\mathrm{Gal}(L/E) = \mathrm{Gal}(L/F) = S_n$. So we must have $E = F$. □

Definition (General polynomial)**.** Let K be a field, $u_1, \cdots, u_n$ variables. The *general polynomial over* K of degree n is

$$f = t^n + u_1t^{n-1} + \cdots + u_n.$$

Technically, this is a polynomial in the polynomial ring $K(u_1, \cdots, u_n)[t]$. However, we say this is the general polynomial over K be cause we tend to think of these u_i as representing actual elements of K.

We say the general polynomial over K of degree n can be solved by radicals if f can be solved by radicals over $K(u_1, \cdots, u_n)$.

Example. The general polynomial of degree 2 over $\mathbb{Q}$ is

$$t^2 + u_1t + u_2.$$

This can be solved by radicals because its roots are

$$\frac{-u_1 \pm \sqrt{u_1^2 - 4u_2}}{2}.$$

Theorem. Let K be a field with $\operatorname{char} K = 0$. Then the general polynomial polynomial over K of degree n cannot be solved by radicals if $n \geq 5$.

Proof. Let
$$f = t^n + u_1 t^{n-1} + \cdots + u_n.$$
be our general polynomial of degree $n \geq 5$. Let N be a splitting field of f over $K(u_1, \cdots, u_n)$. Let
$$\operatorname{Root}_f(N) = \{\alpha_1, \cdots, \alpha_n\}.$$
We know the roots are distinct because f is irreducible and the field has characteristic 0. So we can write
$$f = (t - \alpha_1) \cdots (t - \alpha_n) \in N[t].$$
We can expand this to get
$$\begin{aligned} u_1 &= -(\alpha_1 + \cdots + \alpha_n) \\ u_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n \\ &\vdots \\ u_i &= (-1)^i (i\text{th elementary symmetric polynomial in } \alpha_1, \cdots, \alpha_n). \end{aligned}$$
Now let $x_1, \cdots, x_n$ be new variables, and e_i the ith elementary symmetric polynomial in $x_1, \cdots, x_n$. Let $L = K(x_1, \cdots, x_n)$, and $F = K(e_1, \cdots, e_n)$. We know that $F \subseteq L$ is a Galois extension with Galois group isomorphic to S_n.

We define a ring homomorphism
$$\begin{aligned} \theta : K[u_1, \cdots, u_n] &\to K[e_1, \cdots, e_n] \subseteq K[x_1, \cdots, x_n] \\ u_i &\mapsto (-1)^i e_i. \end{aligned}$$
This is our equations of u_i in terms α_i, but with x_i instead of α_i.

We want to show that θ is an isomorphism. Note that since the homomorphism just renames u_i into e_i, the fact that θ is an isomorphism means there are no "hidden relations" between the e_i. It is clear that θ is a surjection. So it suffices to show θ is injective. Suppose $\theta(h) = 0$. Then
$$h(-e_1, \cdots, (-1)^n e_n) = 0.$$
Since the x_i are just arbitrary variables, we now replace x_i with α_i. So we get
$$h(-e_1(\alpha_1, \cdots, \alpha_n), \cdots, (-1)^n (e_n(\alpha_1, \cdots, \alpha_n))) = 0.$$
Using our expressions for u_i in terms of e_i, we have
$$h(u_1, \cdots, u_n) = 0,$$
But $h(u_1, \cdots, u_n)$ is just h itself. So $h = 0$. Hence θ is injective. So it is an isomorphism. This in turns gives an isomorphism between
$$K(u_1, \cdots, u_n) \to K(e_1, \cdots, e_n) = F.$$
We can extend this to their polynomial rings to get isomorphisms between
$$K(u_1, \cdots, u_n)[t] \to F[t].$$

In particular, this map sends our original f to

$$f \mapsto t^n - e_1 t^{n-1} + \cdots + (-1)^n e_n = g.$$

Thus, we get an isomorphism between the splitting field of f over $K(u_1, \cdots, u_n)$ and the splitting field g over F.

The splitting field of f over $K(u_1, \cdots, u_n)$ is just N by definition. From the symmetric rational function theorem, we know that the splitting field of g over F is just L, and So $N \cong L$. So we have an isomorphism

$$\mathrm{Gal}(N/K(u_1, \cdots, u_n)) \to \mathrm{Gal}(L/F) \cong S_n.$$

Since S_n is not soluble, f is not soluble. □

This is our second main goal of the course, to prove that general polynomials of degree 5 or more are not soluble by radicals.

Recall that we proved that all radical extensions are soluble. We now prove the converse.

Theorem. Let K be a field with $\mathrm{char}\, K = 0$. If L/K is a soluble extension, then it is a radical extension.

Proof. Let $L \subseteq E$ be such that $K \subseteq E$ is Galois and $\mathrm{Gal}(E/K)$ is soluble. We can replace L with E, and assume that in fact L/K is a soluble Galois extension. So there is a sequence of groups

$$\{0\} = G_r \lhd \cdots \lhd G_1 \lhd G_0 = \mathrm{Gal}(L/K)$$

such that G_i/G_{i+1} is cyclic.

By the fundamental theorem of Galois theory, we get a sequence of field extension given by $L_i = L^{G_i}$:

$$K = L_0 \subseteq \cdots \subseteq L_r = L.$$

Moreover, we know that $L_i \subseteq L_{i+1}$ is a Galois extension with Galois group $\mathrm{Gal}(L_{i+1}/L_i) \cong G_i/G_{i+1}$. So $\mathrm{Gal}(L_{i+1}/L_i)$ is cyclic.

Let $n = [L : K]$. Recall that we proved a previous theorem that if $\mathrm{Gal}(L_{i+1}/L_i)$ is cyclic, and L_i contains a primitive kth root of unity (with $k = [L_{i+1} : L_i]$), then $L_i \subseteq L_{i+1}$ is a Kummer extension. However, we do not know of L_i contains the right root of unity. Hence, the trick here is to add an nth primitive root of unity to each field in the sequence.

Let μ an nth primitive root of unity. Then if we add the nth primitive root to each item of the sequence, we have

$$\begin{array}{ccccccccccc}
L_0(\mu) & \subseteq & \cdots & \subseteq & L_i(\mu) & \subseteq & L_{i+1}(\mu) & \subseteq & \cdots & \subseteq & L_r(\mu) \\
\cup| & & & & \cup| & & \cup| & & & & \cup| \\
K = L_0 & \subseteq & \cdots & \subseteq & L_i & \subseteq & L_{i+1} & \subseteq & \cdots & \subseteq & L_r = L
\end{array}$$

We know that $L_0 \subseteq L_0(\mu)$ is a cyclotomic extension by definition. We will now show that $L_i(\mu) \subseteq L_{i+1}(\mu)$ is a Kummer extension for all i. Then L/K is radical since $L \subseteq L_r(\mu)$.

Before we do anything, we have to show $L_i(\mu) \subseteq L_{i+1}(\mu)$ is a Galois extension. To show this, it suffices to show $L_i \subseteq L_{i+1}(\mu)$ is a Galois extension.

Since $L_i \subseteq L_{i+1}$ is Galois, $L_i \subseteq L_{i+1}$ is normal. So L_{i+1} is the splitting of some h over L_i. Then $L_{i+1}(\mu)$ is just the splitting field of $(t^n - 1)h$. So $L_i \subseteq L_{i+1}(\mu)$ is normal. Also, $L_i \subseteq L_{i+1}(\mu)$ is separable since $\operatorname{char} K = \operatorname{char} L_i = 0$. Hence $L_i \subseteq L_{i+1}(\mu)$ is Galois, which implies that $L_i(\mu) \subseteq L_{i+1}(\mu)$ is Galois.

We define a homomorphism of groups

$$\operatorname{Gal}(L_{i+1}(\mu)/L_i(\mu)) \to \operatorname{Gal}(L_{i+1}/L_i)$$

by restriction. This is well-defined because L_{i+1} is the splitting field of some h over L_i, and hence any automorphism of $L_{i+1}(\mu)$ must send roots of h to roots of h, i.e. L_{i+1} to L_{i+1}.

Moreover, we can see that this homomorphism is injective. If $\phi \mapsto \phi|_{L_{i+1}} = \mathrm{id}$, then it fixes everything in L_{i+1}. Also, since it is in $\operatorname{Gal}(L_{i+1}(\mu)/L_i(\mu))$, it fixes $L_i(\mu)$. In particular, it fixes μ. So ϕ must fix the whole of $L_{i+1}(\mu)$. So $\phi = \mathrm{id}$.

By injectivity, we know that $\operatorname{Gal}(L_{i+1}(\mu)/L_i(\mu))$ is isomorphic to a subgroup of $\operatorname{Gal}(L_{i+1}/L_i)$. Hence it is cyclic. By our previous theorem, it follows that $L_i(\mu) \subseteq L_{i+1}(\mu)$ is a Kummer extension. So L/K is radical. □

Corollary. Let K be a field with $\operatorname{char} K = 0$ and $h \in K[t]$. Let L be the splitting of h over K. Then h can be solved by radicals if and only if $\operatorname{Gal}(L/K)$ is soluble.

Proof. ($\Rightarrow$) Proved before.

($\Leftarrow$) Since L/K is a Galois extension, L/K is a soluble extension. So it is a radial extension. So h can be solved by radicals. □

Corollary. Let K be a field with $\operatorname{char} K = 0$. Let $f \in K[t]$ have $\deg f \leq 4$. Then f can be solved by radicals.

Proof. Exercise. □

Note that in the case where $K = \mathbb{Q}$, we have proven this already by given explicit solutions in terms of radicals in the first lecture.

4 Computational techniques

In the last three lectures, we will look at some techniques that allow us to actually compute the Galois group of polynomials (i.e. Galois groups of their splitting fields).

4.1 Reduction mod p

The goal of this chapter is to see what happens when we reduce a polynomial $f \in \mathbb{Z}[t]$ to the corresponding polynomial $\bar{f} \in \mathbb{F}_p[t]$.

More precisely, suppose we have a polynomial $f \in \mathbb{Z}[t]$, and E is its splitting field over $\mathbb{Q}$. We then reduce f to $\bar{f} \in \mathbb{F}_p[t]$ by reducing the coefficients mod p, and let $\bar{E}$ be the splitting field of $\bar{f}$ over $\mathbb{F}_p$.

The ultimate goal is to show that under mild assumptions, there is an injection

$$\mathrm{Gal}(\overline{E}/\mathbb{F}_p) \hookrightarrow \mathrm{Gal}(E/\mathbb{Q}).$$

To do this, we will go through a lot of algebraic fluff to obtain an alternative characterization of the Galois group, and obtain the result as an easy corollary.

This section will be notationally heavy. First, in the background, we have a polynomial f of degree n (whose field we shall specify later). Then we will have three distinct set of variables, namely $(x_1, \cdots, x_n)$, $(u_1, \cdots, u_n)$, plus a t. They will play different roles.

- The x_i will be placeholders. After establishing our definitions, we will then map each x_i to α_i, a root of our f.
- The u_i will stay as "general coefficients" all the time.
- t will be the actual variable we think our polynomial is in, i.e. all polynomials will be variables in t, and u_i and x_i will form part of the coefficients.

To begin with, let

$$L = \mathbb{Q}(x_1, \cdots, x_n)$$
$$F = \mathbb{Q}(e_1, \cdots, e_n).$$

where x_i are variables and e_i are the symmetric polynomials in the $x_1, \cdots, x_n$. We have seen that $\mathrm{Gal}(L/F) \cong S_n$.

Now let

$$B = \mathbb{Z}[x_1, \cdots, x_n]$$
$$A = \mathbb{Z}[e_1, \cdots, e_n].$$

It is an exercise on example sheet 4 to show that

$$B \cap F = A. \tag{$*$}$$

We will for now take this for granted.

We now add it new variables $u_1, \cdots, u_n, t$. We previously mentioned that S_n can act on, say $L[u_1, \cdots, u_n, t]$ by permuting the variables. Here there are two ways in which this can happen — a permutation can either permute the x_i, or permute the u_i. We will have to keep this in mind.

Now for each $\sigma \in S_n$, we define the linear polynomial

$$R_\sigma = t - x_{\sigma(1)}u_1 - \cdots - x_{\sigma(n)}u_n.$$

For example, we have

$$R_{(1)} = t - x_1u_1 - \cdots - x_nu_n.$$

As mentioned, an element $\rho \in S_n$ can act on R_ρ in two ways: it either sends $R_\sigma \mapsto R_{\rho\sigma}$ or $R_\sigma \mapsto R_{\sigma\rho^{-1}}$.

It should be clear that the first action permutes the x_i. What the second action does is permute the u_i. To see this, we can consider a simple case where $n = 2$. Then the action ρ acting on $R_{(1)}$ sends

$$t - x_1u_1 - x_2u_2 \mapsto t - x_{\rho^{-1}(1)}u_1 - x_{\rho^{-2}(2)}u_2 = t - x_1u_{\rho(1)} - x_2u_{\rho(2)}.$$

Finally, we define the following big scary polynomial:

$$R = \prod_{\sigma\in S_n} R_\sigma \in B[u_1, \cdots, u_n, t].$$

We see that this is fixed by any permutation in $\sigma \in S_n$ under both actions. Considering the first action and using $(*)$, we see that in fact

$$R \in A[u_1, \cdots, u_n, t].$$

This is since if we view R as a polynomial over B in the variables $u_1, \cdots, u_n, t$, then its coefficients will be invariant under permuting the x_i. So the coefficients must be a function of the e_i, i.e. lie in A.

With these definitions in place, we can focus on a concrete polynomial.

Let K be a field, and let

$$f = t^n + a_1t^{n-1} + \cdots + a_n \in K[t]$$

have no repeated roots. We let E be the splitting field of f over K. Write

$$\mathrm{Root}_f(E) = \{\alpha_1, \cdots, \alpha_n\}.$$

Note that this is the setting we had at the beginning of the chapter, but with an arbitrary field K instead of $\mathbb{Q}$ and $\mathbb{F}_p$.

We define a ring homomorphism $\theta : B \to E$ by $x_i \mapsto \alpha_i$. This extends to a ring homomorphism

$$\theta : B[u_1, \cdots, u_n, t] \to E[u_1, \cdots, u_n, t].$$

Note that the ring homomorphism θ send $e_i \mapsto (-1)^i a_i$. So in particular, if we restrict the homomorphism θ to A, then the image is restricted to the field generated by a_i. But we already have $a_i \in K$. So $\theta(A) = K$. In particular, since $R \in A[u_1, \cdots, u_n, t]$, we have

$$\theta(R) \in K[u_1, \cdots, u_n, t].$$

Now let P be an irreducible factor of $\theta(R)$ in $K[u_1, \cdots, u_n, t]$. We want to say each such irreducible polynomial is related to the Galois group $G = \mathrm{Gal}(E/K)$.

Since f has no repeated roots, we can consider G as a subgroup of S_n, where the elements of G are just the permutations of the roots α_i. We will then show that each irreducible polynomial corresponds to a coset of G.

Recall that at the beginning, we said S_n can act on our polynomial rings by permuting the x_i or u_i. However, once we have mapped the x_i to the α_i and focus on a specific field, S_n as a whole can no longer act on the α_i, since there might be non-trivial relations between the α_i. Instead, only the subgroup $G \leq S_n$ can act on α_i. On the other hand, S_n can still act on u_i.

Recall that R is defined as a product of linear factors R_σ's. So we can find a subset $\Lambda \subseteq S_n$ such that

$$P = \prod_{\sigma \in \Lambda} R_\sigma.$$

We will later see this Λ is just a coset of the Galois group G.

Pick $\sigma \in \Lambda$. Then by definition of P,

$$R_\sigma \mid P$$

in $E[u_1, \cdots, u_n, t]$. Now if $\rho \in G$, then we can let ρ act on both sides by permuting the x_i (i.e. the α_i). This does not change P because P has coefficients in K and the action of G has to fix K. Hence we have

$$R_{\rho\sigma} \mid P.$$

More generally, if we let

$$H = \prod_{\rho \in G} R_{\rho\sigma} \in E[u_1, \cdots, u_n, t],$$

then

$$H \mid P$$

by the irreducibility of P.

Since H is also invariant under the action of G, we know $H \in K[u_1, \cdots, u_n, t]$. By the irreducibility of P, we know $H = P$. Hence, we know

$$\Lambda = G\sigma.$$

We have thus proved that the irreducible factors of $\theta(R)$ in $K[u_1, \cdots, u_n, t]$ are in one-to-one correspondence with the cosets of G in S_n. In particular, if P corresponds to G itself, then

$$P = \prod_{\tau \in G} R_\tau.$$

In general, if P corresponds to a coset $G\sigma$, we can let $\lambda \in S_n$ act on P by permuting the u_i's. Then this sends

$$P = \prod_{\rho \in G} R_{\rho\sigma} \mapsto Q = \prod_{\rho \in G} R_{\rho\sigma\lambda^{-1}}.$$

So this corresponds to the coset $G\sigma\lambda^{-1}$. In particular, $P = Q$ if and only if $G\sigma = G\sigma\lambda^{-1}$. So we can use this to figure out what permutations preserve an irreducible factor. In particular, taking $\sigma = (1)$, we have

Theorem.

$$G = \{\lambda \in S_n : \lambda \text{ preserves the irreducible factor corresponding to } G\}. \quad (\dagger)$$

This is the key result of this chapter, and we will apply this as follows:

Theorem. Let $f \in \mathbb{Z}[t]$ be monic with no repeated roots. Let E be the splitting field of f over $\mathbb{Q}$, and take $\bar{f} \in \mathbb{F}_p[t]$ be the obvious polynomial obtained by reducing the coefficients of f mod p. We also assume this has no repeated roots, and let $\bar{E}$ be the splitting field of $\bar{f}$.

Then there is an injective homomorphism

$$\bar{G} = \mathrm{Gal}(\bar{E}/\mathbb{F}_p) \hookrightarrow G = \mathrm{Gal}(E/\mathbb{Q}).$$

Moreover, if $\bar{f}$ factors as a product of irreducibles of length $n_1, n_2, \cdots, n_r$, then $\mathrm{Gal}(f)$ contains an element of cycle type $(n_1, \cdots, n_r)$.

Proof. We apply the previous theorem twice. First, we take $K = \mathbb{Q}$. Then

$$\theta(R) \in \mathbb{Z}[u_1, \cdots, u_n, t].$$

Let P be the irreducible factor of $\theta(R)$ corresponding to the Galois group G. Applying Gauss' lemma, we know P has integer coefficients.

Applying the theorem again, taking $K = \mathbb{F}_p$. Denote the ring homomorphism as $\bar{\theta}$. Then $\bar{\theta}(R) \in \mathbb{F}_p[u_1, \cdots, u_n, t]$. Now let Q be the irreducible factor $\bar{\theta}(R)$ corresponding to $\bar{G}$.

Now note that $\theta(R_{(1)}) \mid P$ and $\bar{\theta}(R_{(1)}) \mid Q$, since the identity is in G and $\bar{G}$. Also, note that $\bar{\theta}(R) = \overline{\theta(R)}$, where the bar again denotes reduction mod p. So $Q \mid \bar{P}$.

Considering the second action of S_n (i.e. permuting the u_i), we can show $\bar{G} \subseteq G$, using the characterization (†). Details are left as an exercise. □

This is incredibly useful for computing Galois groups, as it allows us to explicitly write down some cycles in $\mathrm{Gal}(E, \mathbb{Q})$.

4.2 Trace, norm and discriminant

We are going to change direction a bit and look at traces and norms. These will help us understand the field better, and perhaps prove some useful facts from it. They will also lead to the notion of the discriminant, which is again another tool that can be used to compute Galois groups, amongst many other things.

Definition (Trace)**.** Let K be a field. If $A = [a_{ij}]$ is an $n \times n$ matrix over K, we define the *trace* of A to be

$$\mathrm{tr}(A) = \sum_{i=1}^{n} a_{ii},$$

i.e. we take the sum of the diagonal terms.

It is a well-known fact that if B is an invertible $n \times n$ matrix, then

$$\mathrm{tr}(B^{-1}AB) = \mathrm{tr}(A).$$

Hence given a finite-dimensional vector space V over K and $\sigma : V \to V$ a K-linear map, then we can define the trace for the linear map as well.

Definition (Trace of linear map)**.** Let V be a finite-dimensional vector space over K, and $\sigma : V \to V$ a K-linear map. Then we can define

$$\mathrm{tr}(\sigma) = \mathrm{tr}(\text{any matrix representing } \sigma).$$

Definition (Trace of element)**.** Let $K \subseteq L$ be a finite field extension, and $\alpha \in L$. Consider the K-linear map $\sigma : L \to L$ given by multiplication with α, i.e. $\beta \mapsto \alpha\beta$. Then we define the *trace* of α to be

$$\mathrm{tr}_{L/K}(\alpha) = \mathrm{tr}(\sigma).$$

Similarly, we can consider the determinant, and obtain the norm.

Definition (Norm of element)**.** We define the *norm* of α to be

$$N_{L/K}(\alpha) = \det(\sigma),$$

where σ is, again, the multiplication-by-α map.

This construction gives us two functions $\mathrm{tr}_{L/K}, N_{L/K} : L \to K$. It is easy to see from definition that $\mathrm{tr}_{L/K}$ is additive while $N_{L/K}$ is multiplicative.

Example. Let L/K be a finite field extension, and $x \in K$. Then the matrix of x is represented by xI, where I is the identity matrix. So

$$N_{L/K}(x) = x^{[L:K]}, \quad \mathrm{tr}_{L/K}(x) = [L : K]x.$$

Example. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$. Consider an element $a + bi \in \mathbb{Q}(i)$, and pick the basis $\{1, i\}$ for $\mathbb{Q}(i)$. Then the matrix of $a + bi$ is

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

So we find that $\mathrm{tr}_{L/K}(a + bi) = 2a$ and $N(a + bi) = a^2 + b^2 = |a + bi|^2$.

In general, if $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{-d})$ where $d > 0$ is square-free, then $N(a + b\sqrt{-d}) = a^2 + b^2 d = |a + b\sqrt{-d}|^2$. However, for other fields, the norm is not at all related to the absolute value.

In general, computing norms and traces with the definition directly is not fun. It turns out we can easily find the trace and norm of α from the minimal polynomial of α, just like how we can find usual traces and determinants from the characteristic polynomial.

To do so, we first prove the transitivity of trace and norm.

Lemma. Let $L/F/K$ be finite field extensions. Then

$$\mathrm{tr}_{L/K} = \mathrm{tr}_{F/K} \circ \mathrm{tr}_{L/F}, \quad N_{L/K} = N_{F/K} \circ N_{L/F}.$$

To prove this directly is not difficult, but involves some confusing notation. Purely for the sake of notational convenience, we shall prove the following more general fact:

Lemma. Let F/K be a field extension, and V an F-vector space. Let $T : V \to V$ be an F-linear map. Then it is in particular a K-linear map. Then

$$\det_K T = N_{F/K}(\det_F T), \quad \mathrm{tr}_K T = \mathrm{tr}_{F/K}(\mathrm{tr}_F T).$$

Taking V to be L and T to be multiplication by $\alpha \in F$ clearly gives the original intended result.

Proof. For $\alpha \in F$, we will write $m_\alpha : F \to F$ for multiplication by α map viewed as a K-linear map.

By IB Groups, Rings and Modules, there exists a basis $\{e_i\}$ such that T is in rational canonical form, i.e. such that T is block diagonal with each diagonal looking like

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{r-1} \end{pmatrix}.$$

Since the norm is multiplicative and trace is additive, and

$$\det \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \det A \det B, \quad \operatorname{tr} \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \operatorname{tr} A + \operatorname{tr} B,$$

we may wlog T is represented by a single block as above.

From the rational canonical form, we can read off

$$\det_F T = (-1)^{r-1} a_0, \quad \operatorname{tr}_F T = a_{r-1}.$$

We now pick a basis $\{f_j\}$ of F over K, and then $\{e_i f_j\}$ is a basis for V over K. Then in this basis, the matrix of T over K is given by

$$\begin{pmatrix} \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & m_{a_0} \\ \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} & m_{a_1} \\ \mathbf{0} & \mathbf{1} & \cdots & \mathbf{0} & m_{a_2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{1} & m_{a_{r-1}} \end{pmatrix}.$$

It is clear that this has trace

$$\operatorname{tr}_K(m_{a_{r-1}}) = \operatorname{tr}_{F/K}(a_{r-1}) = \operatorname{tr}_{F/K}(\operatorname{tr}_F T).$$

Moreover, writing $n = [L : K]$, we have

$$\begin{aligned} \det_K \begin{pmatrix} \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & m_{a_0} \\ \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} & m_{a_1} \\ \mathbf{0} & \mathbf{1} & \cdots & \mathbf{0} & m_{a_2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{1} & m_{a_{r-1}} \end{pmatrix} &= (-1)^{n(r-1)} \det_K \begin{pmatrix} m_{a_0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ m_{a_1} & \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} \\ m_{a_2} & \mathbf{0} & \mathbf{1} & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m_{a_{r-1}} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{1} \end{pmatrix} \\ &= (-1)^{n(r-1)} \det_K(m_{a_0}) \\ &= \det_K((-1)^{r-1} m_{a_0}) \\ &= N_{F/K}((-1)^{r-1} a_0) \\ &= N_{F/K}(\det_F T). \end{aligned}$$

So the result follows. □

As a corollary, we have the following very powerful tool for computing norms and traces.

Corollary. Let L/K be a finite field extension, and $\alpha \in L$. Let $r = [L : K(\alpha)]$ and let P_α be the minimal polynomial of α over K, say

$$P_\alpha = t^n + a_{n-1}t^{n-1} + \cdots + a_0.$$

with $a_i \in K$. Then

$$\mathrm{tr}_{L/K}(\alpha) = -ra_{n-1}$$

and

$$N_{L/K}(\alpha) = (-1)^{nr}a_0^r.$$

Note how this resembles the relation between the characteristic polynomial and trace/determinants in linear algebra.

Proof. We first consider the case $r = 1$. Write m_α for the matrix representing multiplication by α. Then P_α is the minimal polynomial of m_α. But since $\deg P_\alpha = n = \dim_K K(\alpha)$, it follows that this is also the characteristic polynomial. So the result follows.

Now if $r \neq 1$, we can consider the tower of extensions $L/K(\alpha)/K$. Then we have

$$\begin{aligned} N_{L/K}(\alpha) = N_{K(\alpha)/K}(N_{L/K(\alpha)}(\alpha)) &= N_{K(\alpha)/K}(\alpha^r) \\ &= (N_{K(\alpha)/K}(\alpha))^r = (-1)^{nr}a_0^r. \end{aligned}$$

The computation for trace is similar. □

It is also instructive to prove this directly. In the case $r = 1$, we can pick the basis $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ of L over K. Then the multiplication map sends

$$\begin{aligned} 1 &\mapsto \alpha \\ \alpha &\mapsto \alpha^2 \\ &\vdots \\ \alpha^{n-1} &\mapsto \alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0 \end{aligned}$$

So the matrix is just

$$A = \begin{pmatrix} 0 & 0 & \cdots & -a_0 \\ 1 & 0 & \cdots & -a_1 \\ 0 & 1 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -a_{n-1} \end{pmatrix}$$

The characteristic polynomial of this matrix is

$$\det(tI - A) = \det \begin{pmatrix} t & 0 & \cdots & a_0 \\ -1 & t & \cdots & a_1 \\ 0 & -1 & \cdots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & t + a_{n-1} \end{pmatrix}$$

By adding t^i multiples of the ith row to the first row for each i, this gives

$$\det(tI - A) = \det \begin{pmatrix} 0 & 0 & \cdots & P_\alpha \\ -1 & t & \cdots & a_1 \\ 0 & -1 & \cdots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & t + a_{n-1} \end{pmatrix} = P_\alpha.$$

Then we notice that for $r \neq 1$, in an appropriate choice of basis, the matrix looks like

$$C = \begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A \end{pmatrix}.$$

Theorem. Let L/K be a finite but not separable extension. Then $\mathrm{tr}_{L/K}(\alpha) = 0$ for all $\alpha \in L$.

Proof. Pick $\beta \in L$ such that P_β, the minimal polynomial of β over K, is not separable. Then by the previous characterization of separable polynomials, we know $p = \mathrm{char}\, K > 0$ with $P_\beta = q(t^p)$ for some $q \in K[t]$.

Now consider

$$K \subseteq K(\beta^p) \subseteq K(\beta) \subseteq L.$$

To show $\mathrm{tr}_{L/K} = 0$, by the previous proposition, it suffices to show $\mathrm{tr}_{K(\beta)/K(\beta^p)} = 0$.

Note that the minimal polynomial of β^p over K is q because $q(\beta^p) = 0$ and q is irreducible. Then $[K(\beta) : K] = \deg P_\beta = p \deg q$ and $\deg[K(\beta^p) : K] = \deg q$. So $[K(\beta) : K(\beta^p)] = p$.

Now $\{1, \beta, \beta^2, \cdots, \beta^{p-1}\}$ is a basis of $K(\beta)$ over $K(\beta^p)$. Let R_{β^i} be the minimal polynomial of β^i over $K(\beta^p)$. Then

$$R_{\beta^i} = \begin{cases} t - 1 & i = 0 \\ t^p - \beta^{ir} & i \neq 0 \end{cases},$$

We get the second case using the fact that p is a prime number, and hence $K(\beta^p)(\beta^i) = K(\beta)$ if $1 \leq i < p$. So $[K(\beta^p)(\beta^i) : K(\beta^p)] = p$ and hence the minimal polynomial has degree p. Hence $\mathrm{tr}_{K(\beta)/K(\beta^p)}(\beta^i) = 0$ for all i.

Thus, $\mathrm{tr}_{K(\beta)/K(\beta^p)} = 0$. Hence

$$\mathrm{tr}_{L/K} = \mathrm{tr}_{K(\beta^p)/K} \circ \mathrm{tr}_{K(\beta)/K(\beta^p)} \circ \mathrm{tr}_{L/K(\beta)} = 0. \qquad \square$$

Note that if L/K is a finite extension, and $\mathrm{char}\, K = 0$, then

$$\mathrm{tr}_{L/K}(1) = [L : K] \neq 0.$$

So $\mathrm{tr}_{L/K} \neq 0$. It is in fact true that all separable extensions have $\mathrm{tr}_{L/K} \neq 0$, not only when the field has characteristic 0.

Example. We want to show $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$. Suppose not. Then we have $L = \mathbb{Q}(\sqrt[3]{3}) = \mathbb{Q}(\sqrt[3]{2})$, since both extensions of $\mathbb{Q}$ have degree 3. Then there exists some $a, b, c \in \mathbb{Q}$ such that

$$\sqrt[3]{3} = a + b\sqrt[3]{2} + c\sqrt[3]{2^2}.$$

We now compute the traces over $\mathbb{Q}$. The minimal polynomials over $\mathbb{Q}$ are

$$P_{\sqrt[3]{3}} = t^3 - 3, \quad P_{\sqrt[3]{2}} = t^3 - 2, \quad P_{\sqrt[3]{4}} = t^3 - 4.$$

So we have

$$\operatorname{tr}_{L/\mathbb{Q}}(\sqrt[3]{3}) = a \operatorname{tr}_{L/\mathbb{Q}}(1) + b \operatorname{tr}_{L/\mathbb{Q}}(\sqrt[3]{2}) + c \operatorname{tr}_{L/\mathbb{Q}}(\sqrt[3]{4}).$$

Since the minimal polynomials above do not have coefficients in t^2, the traces of the cube roots are zero. So we need $a = 0$. Then we are left with

$$\sqrt[3]{3} = b\sqrt[3]{2} + c\sqrt[3]{4}.$$

We apply the same trick again. We multiply by $\sqrt[3]{2}$ to obtain

$$\sqrt[3]{6} = b\sqrt[3]{4} + 2c.$$

We note that the minimal polynomial of $\sqrt[3]{6}$ is $t^3 - 6$. Taking the trace gives

$$\operatorname{tr}_{L/\mathbb{Q}}(\sqrt[3]{6}) = b \operatorname{tr}_{L/\mathbb{Q}}(\sqrt[3]{4}) + 6c.$$

Again, the traces are zero. So $c = 0$. So we have

$$\sqrt[3]{3} = b\sqrt[3]{2}.$$

In other words,

$$b^3 = \frac{3}{2},$$

which is clearly nonsense. This is a contradiction. So $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$.

We can obtain another formula for the trace and norm as follows:

Theorem. Let L/K be a finite separable extension. Pick a further extension E/L such that E/K is normal and

$$|\operatorname{Hom}_K(L, E)| = [L : K].$$

Write $\operatorname{Hom}_K(L, E) = \{\varphi_1, \cdots, \varphi_n\}$. Then

$$\operatorname{tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \varphi_i(\alpha), \quad N_{L/K}(\alpha) = \prod_{i=1}^{n} \varphi_i(\alpha)$$

for all $\alpha \in L$.

Proof. Let $\alpha \in L$. Let P_α be the minimal polynomial of α over K. Then there is a one-to-one correspondence between

$$\operatorname{Hom}_K(K(\alpha), E) \longleftrightarrow \operatorname{Root}_{P_\alpha}(E) = \{\alpha_1, \cdots, \alpha_d\}.$$

wlog we let $\alpha = \alpha_1$.

Also, since

$$|\operatorname{Hom}_K(L, E)| = [L : K],$$

we get

$$|\operatorname{Hom}_K(K(\alpha), E)| = [K(\alpha) : K] = \deg P_\alpha.$$

Moreover, the restriction map $\mathrm{Hom}_K(L, E) \to \mathrm{Hom}_K(K(\alpha), E)$ (defined by $\varphi \mapsto \varphi|_{K(\alpha)}$) is surjective and sends exactly $[K(\alpha) : K]$ elements to any particular element in $\mathrm{Hom}_K(K(\alpha), E)$.

Therefore

$$\sum \varphi_i(\alpha) = [L : K(\alpha)] \sum_{\psi \in \mathrm{Hom}_K(K(\alpha), E)} \psi(\alpha) = [L : K(\alpha)] \sum_{i=1}^{d} \alpha_i.$$

Moreover, we can read the sum of roots of a polynomial is the (negative of the) coefficient of t^{d-1}, where

$$P_\alpha = t^d + a_{d-1}t^{d-1} + \cdots + a_0.$$

So

$$\sum \varphi_i(\alpha) = [L : K(\alpha)](-a_{d-1}) = \mathrm{tr}_{L/K}(\alpha).$$

Similarly, we have

$$\begin{aligned}
\prod \varphi_i(\alpha) &= \left(\prod_{\psi \in \mathrm{Hom}_K(K(\alpha), E)} \psi(\alpha) \right)^{[L:K(\alpha)]} \\
&= \left(\prod_{i=1}^{d} \alpha_i \right)^{[L:K(\alpha)]} \\
&= ((-1)^d a_0)^{[L:K(\alpha)]} \\
&= N_{L/K}(\alpha).
\end{aligned}$$

□

Corollary. Let L/K be a finite separable extension. Then there is some $\alpha \in L$ such that $\mathrm{tr}_{L/K}(\alpha) \neq 0$.

Proof. Using the notation of the previous theorem, we have

$$\mathrm{tr}_{L/K}(\alpha) = \sum \varphi_i(\alpha).$$

Similar to a previous lemma, we can show that $\varphi_1, \cdots, \varphi_n$ are "linearly independent" over E, and hence $\sum \varphi_i$ cannot be identically zero. Hence there is some α such that

$$\mathrm{tr}_{L/K}(\alpha) = \sum \varphi_i(\alpha) \neq 0.$$

□

Example. Let $K = \mathbb{F}_q \subseteq L = \mathbb{F}_{q^n}$, with q is a power of some prime number p. By a previous theorem on finite fields, we know L/K is Galois and

$$\mathrm{Gal}(L/K) = \frac{\mathbb{Z}}{n\mathbb{Z}}$$

and is generated by the Frobenius $\varphi = \mathrm{Fr}_q$.

To apply the theorem, we had to pick an E such that E/K is normal and $\mathrm{Hom}_K(L, E) = [L : K]$. However, since L/K is Galois, we can simply pick $E = L$.

Then we know

$$\begin{aligned}\mathrm{tr}_{L/K}(\alpha) &= \sum_{\psi \in \mathrm{Gal}(L/K)} \psi(\alpha)\\ &= \sum_{i=0}^{n-1} \varphi^i(\alpha)\\ &= \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}}.\end{aligned}$$

Similarly, the norm is

$$N_{L/K}(\alpha) = \prod_{i=0}^{n-1} \varphi^i(\alpha) = \alpha \cdot \alpha^q \cdot \cdots \cdot \alpha^{q^{n-1}}.$$

Recall that when solving quadratic equations $f = t^2 + bt + c$, we defined the *discriminant* as $b^2 - 4c$. This discriminant then determined the types of roots of f. In general, we can define the discriminant of a polynomial of any degree, in a scary way.

Definition (Discriminant)**.** Let K be a field and $f \in K[t]$, L the splitting field of f over K. So we have

$$f = a(t - \alpha_1) \cdots (t - \alpha_n)$$

for some $a, \alpha_1, \cdots, \alpha_n \in L$. We define

$$\Delta_f = \prod_{i<j} (\alpha_i - \alpha_j), \quad D_f = \Delta_f^2 = (-1)^{n(n-1)/2} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

We call D_f the *discriminant* of f.

Clearly, $D_f \neq 0$ if and only if f has no repeated roots.

Theorem. Let K be a field and $f \in K[t]$, L is the splitting field of f over K. Suppose $D_f \neq 0$ and $\mathrm{char}\, K \neq 2$. Then

(i) $D_f \in K$.

(ii) Let $G = \mathrm{Gal}(L/K)$, and $\theta : G \to S_n$ be the embedding given by the permutation of the roots. Then $\mathrm{im}\, \theta \subseteq A_n$ if and only if $\Delta_f \in K$ (if and only if D_f is a square in K).

Proof.

(i) It is clear that D_f is fixed by $\mathrm{Gal}(L/K)$ since it only permutes the roots.

(ii) Consider a permutation $\sigma \in S_n$ of the form $\sigma = (\ell\ m)$, and let it act on the roots. Then we claim that

$$\sigma(\Delta_f) = -\Delta_f. \tag{$\dagger$}$$

So in general, odd elements in S_n negate Δ_f while even elements fix it. Thus, $\Delta_f \in K$ iff Δ_f is fixed by $\mathrm{Gal}(L/K)$ iff every element of $\mathrm{Gal}(L/K)$ is even.

To prove (†), we have to painstakingly check all terms in the product. We wlog $\ell < m$. If $k < \ell, m$. Then this swaps $(\alpha_k - \alpha_\ell)$ with $\alpha_k - \alpha_m)$, which has no effect. The $k > m$ case is similar. If $\ell < k < m$, then this sends $(\alpha_\ell - \alpha_k) \mapsto (\alpha_m - \alpha_k)$ and $(\alpha_k - \alpha_m) \mapsto (\alpha_\ell - \alpha_m)$. This introduces two negative signs, which has no net effect. Finally, this sends $(\alpha_k - \alpha_m)$ to its negation, and so introduces a negative sign. □

We will later use this result to compute certain Galois groups. Before that, we see how this discriminant is related to the norm.

Theorem. Let K be a field, and $f \in K[t]$ be an n-degree monic irreducible polynomial with no repeated roots. Let L be the splitting field of f over K, and let $\alpha \in \mathrm{Root}_F(L)$. Then

$$D_f = (-1)^{n(n-1)/2} N_{K(\alpha)/K}(f'(\alpha)).$$

Proof. Let $\mathrm{Hom}_K(K(\alpha), L) = \{\varphi_1, \cdots, \varphi_n\}$. Recall these are in one-to-one correspondence with $\mathrm{Root}_f(L) = \{\alpha_1, \cdots, \alpha_n\}$. Then we can compute

$$\prod_{i \neq j} (\alpha_i - \alpha_j) = \prod_i \prod_{j \neq i} (\alpha_i - \alpha_j).$$

Note that since f is just monic, we have

$$f = (t - \alpha_1) \cdots (t - \alpha_n).$$

Computing the derivative directly, we find

$$\prod_{j \neq i} (\alpha_i - \alpha_j) = f'(\alpha_i).$$

So we have

$$\prod_{i \neq j} (\alpha_i - \alpha_j) = \prod_i f'(\alpha_i).$$

Now since the φ_i just maps α to α_i, we have

$$\prod_{i \neq j} (\alpha_i - \alpha_j) = \prod_i \varphi_i(f'(\alpha)) = N_{K(\alpha)/K}(f'(\alpha)).$$

Finally, multiplying the factor of $(-1)^{n(n-1)/2}$ gives the desired result. □

Example. Let K be a field with $\mathrm{char}\, K \neq 2, 3$. Let $f \in K[t]$ have degree 3, say

$$f = t^3 + bt + c$$

where we have gotten rid of the t^2 term as in the first lecture. We further assume f is irreducible with no repeated roots, and let L be the splitting field of f.

We want to compute the discriminant of this polynomial. Let $\alpha \in \mathrm{Root}_f(L)$. Then

$$\beta = f'(\alpha) = 3\alpha^2 + b.$$

Then we can see

$$\beta = -2b - \frac{3c}{\alpha}.$$

Alternatively, we have

$$\alpha = \frac{-3c}{\beta + 2b}. \qquad (*)$$

Putting $(*)$ into $\alpha^3 + b\alpha + c = 0$, we find the minimal polynomial of β has constant term $-4b^3 - 27c^2$. This then gives us the norm, and we get

$$D_f = -N_{K(\alpha)/K}(\beta) = -4b^3 - 27c^2.$$

This is the discriminant of a cubic.

We can take a specific example, where

$$f = t^3 - 31t + 62.$$

Then f is irreducible over $\mathbb{Q}$. We can compute D_f, and find that it is a square. So the previous theorem says the image of the Galois group $\mathrm{Gal}(L/K)$ is a subgroup of A_3. However, we also know $\mathrm{Gal}(L/K)$ has three elements since $\deg f = 3$. So we know $\mathrm{Gal}(L/K) \cong A_3$.